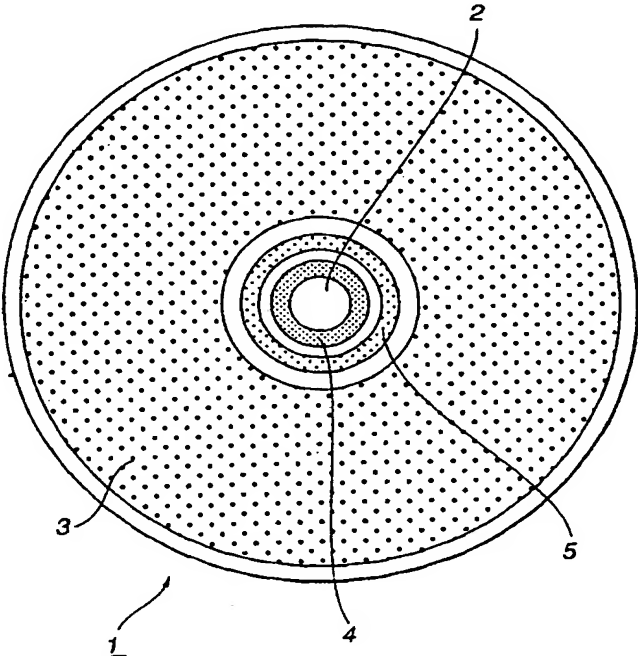


PCT

世界知的所有権機関  
国際事務局  
特許協力条約に基づいて公開された国際出願

(51) 国際特許分類7 G11B 20/10	A1	(11) 国際公開番号 WO00/46804  (43) 国際公開日 2000年8月10日(10.08.00)
<p>(21) 国際出願番号 PCT/JP00/00658</p> <p>(22) 国際出願日 2000年2月7日(07.02.00)</p> <p>(30) 優先権データ 特願平11/30600 1999年2月8日(08.02.99) JP</p> <p>(71) 出願人 (米国を除くすべての指定国について) ソニー株式会社(SONY CORPORATION)[JP/JP] 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo, (JP)</p> <p>(72) 発明者; および</p> <p>(75) 発明者/出願人 (米国についてのみ) 浅野智之(ASANO, Tomoyuki)[JP/JP] 大澤義知(OSAWA, Yoshitomo)[JP/JP] 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo, (JP)</p> <p>(74) 代理人 小池 晃, 外(KOIKE, Akira et al.) 〒105-0001 東京都港区虎ノ門二丁目6番4号 第11森ビル Tokyo, (JP)</p>		<p>(81) 指定国 JP, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE)</p> <p>添付公開書類 国際調査報告書</p>
<p>(54) Title: INFORMATION RECORDING/REPRODUCING SYSTEM</p> <p>(54) 発明の名称 情報記録再生システム</p> <p>(57) Abstract Provided on an information recording medium (1) are a user data recording section (3) on which user data is recorded, a random pattern information recording section (4) on which random pattern information is recorded by making use of a random physical phenomenon, and an authentication data recording section (5) on which medium identifying information generated according to the random pattern information detected from the random pattern information recording section (4) and the digital signatures of manufacturers of the medium identification information are recorded as authentication data.</p> 		

BEST AVAILABLE COPY

(57)要約

情報記録媒体 1 上に、ユーザデータが記録されるユーザデータ記録部 3 と、ランダムな物理現象によるランダムパターン情報が記録されたランダムパターン情報記録部 4 と、上記ランダムパターン情報記録部 4 から検出されるランダムパターン情報に基づいて生成された媒体識別情報と、上記媒体識別情報に対する製造者毎のデジタル署名が認証データとして記録された認証データ記録部 5 とを設ける。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE	アラブ首長国連邦	DM	ドミニカ	KZ	カザフスタン	RU	ロシア
AG	アンティグア・バーブーダ	DZ	アルジェリア	LC	セントルシア	SD	スーダン
AL	アルバニア	EE	エストニア	LI	リヒテンシュタイン	SE	スウェーデン
AM	アルメニア	ES	スペイン	LK	スリ・ランカ	SG	シンガポール
AT	オーストリア	FI	フィンランド	LR	リベリア	SI	スロヴェニア
AU	オーストラリア	FR	フランス	LS	レソト	SK	スロヴァキア
AZ	アゼルバイジャン	GA	ガボン	LT	リトアニア	SL	シエラ・レオネ
BA	ボスニア・ヘルツェゴビナ	GB	英国	LU	ルクセンブルグ	SN	セネガル
BB	バルバドス	GD	グレナダ	LV	ラトヴィア	SZ	スワジランド
BE	ベルギー	GE	グルジア	MA	モロッコ	TD	チャード
BF	ブルキナ・ファソ	GH	ガーナ	MC	モナコ	TG	トーゴ
BG	ブルガリア	GM	ガンビア	MD	モルドヴァ	TJ	タジキスタン
BJ	ベナン	GN	ギニア	MG	マダガスカル	TM	トルクメニスタン
BR	ブラジル	GR	ギリシャ	MK	マケドニア旧ユーゴスラヴィア	TR	トルコ
BY	ベラルーシ	GW	ギニア・ビサウ		共和国	TT	トリニダード・トバゴ
CA	カナダ	HR	クロアチア	ML	マリ	TZ	タンザニア
CF	中央アフリカ	HU	ハンガリー	MN	モンゴル	UA	ウクライナ
CG	コンゴ	ID	インドネシア	MR	モリタニア	UG	ウガンダ
CH	スイス	IE	アイルランド	MW	マラウイ	US	米国
CI	コートジボアール	IL	イスラエル	MX	メキシコ	UZ	ウズベキスタン
CM	カメルーン	IN	インド	MZ	モザンビーク	VN	ヴェトナム
CN	中国	IS	アイスランド	NE	ニジェール	YU	ユーゴスラヴィア
CR	コスタ・リカ	IT	イタリア	NL	オランダ	ZA	南アフリカ共和国
CU	キューバ	JP	日本	NO	ノルウェー	ZW	ジンバブエ
CY	キプロス	KE	ケニア	NZ	ニュージーランド		
CZ	チェッコ	KG	キルギスタン	PL	ポーランド		
DE	ドイツ	KP	北朝鮮	PT	ポルトガル		
DK	デンマーク	KR	韓国	RO	ルーマニア		

## 明細書

### 情報記録再生システム

#### 技術分野

本発明は、記録可能媒体に対する不正コピーを防止するようにした情報記録再生システム、情報記録装置、情報再生装置、認証データ記録装置、認証処理装置、情報記録再生方法、情報記録方法、情報再生方法、認証データの記録方法、情報記録媒体の認証方法及び情報記録媒体に関する。

#### 背景技術

近年、家庭内において音楽情報や映像情報などのデジタルデータを伝送したり記録したりする機器が広く普及している。これらの機器では、データを高品質で記録／再生することが可能であることから、何度複製しても品質劣化のない記録システムを構成することができる。このような記録システムでは、著作権のあるデータが不正にコピーされてしまうのを防止する著作権保護機能を装備する必要がある。

このような著作権保護のためのシステムとして、例えば、Digita

1 Video Disc(DVD) ROM におけるコンテンツスクランブルシステムがある。

このシステムでは、ディスク上の著作権付きデータをすべて暗号化し、ライセンスを受けた機器だけが、暗号を復号して意味のあるデータを得るための暗号鍵を与えられるようにしている。ライセンスを受けた機器は、不正コピーを行わないなどの動作規定に従うように設計されている。

しかし、上述の如きDVDシステムが採用している方式は、読取専用媒体（ROMメディア）に対して有効であるが、ユーザがデータを記録可能な記録可能媒体においては有効でない。なぜならば、RAMメディアにおいては、不正者は、暗号を解読できないとしても、ディスク上のデータを全部、新しいディスクにコピーすることによって、正当な機器で動作するディスクを新たに作ることができるからである。

#### 発明の開示

そこで、本発明の目的は、RAMメディアに対しても有効な不正コピー防止システムを構築した情報記録再生システム、情報記録装置、情報再生装置、認証データ記録装置、認証処理装置、情報記録再生方法、情報記録方法、情報再生方法、認証データの記録方法、情報記録媒体の認証方法及び情報記録媒体を提供することにある。

本発明は、情報を記録し、再生する情報記録再生システムであって、情報記録媒体上のランダムな物理現象によるランダムパターン

情報を記録したランダムパターン情報記録部からランダムな物理現象によるランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報を生成して、上記媒体識別情報を認証データとして上記情報記録媒体上の認証データ記録部に記録する制御を行う認証データ記録制御部と、上記ランダムパターン情報記録部から上記ランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報検査データを生成するとともに、上記情報記録媒体上の認証データ記録部から認証データを読み出し、上記ランダムパターン情報から生成した媒体識別情報検査データと上記認証データに基づいて上記情報記録媒体に対する認証処理を行う認証処理部と、上記認証処理部の認証結果に基づいて、情報記録媒体への情報記録及び情報記録媒体からの情報再生の制御を行う情報記録再生制御部とを具備することを特徴とする。

また、本発明は、ランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部と、上記ランダムパターン情報記録部から検出されるランダムパターン情報に基づいて生成された媒体識別情報を認証データとして格納した認証データ記録部とを有する情報記録媒体に情報を記録する情報記録装置であって、情報記録媒体上のランダムパターン情報記録部からランダムパターン情報を検出するランダムパターン情報検出部と、上記ランダムパターン情報検出部により検出されたランダムパターン情報から媒体識別情報検査データを生成する検査データ生成部と、情報記録媒体上の認証データ記録部から認証データを読み出し、上記検査データ生成部により生成された媒体識別情報検査データと上記認証データに基づいて、情報記録媒体に対する認証処理を行い、認証結果に基

づいて情報の情報記録媒体への書き込みの可否を制御する認証処理部と、情報を情報記録媒体に記録する制御を行う記録制御部とを具備することを特徴とする。

また、本発明は、ランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部と、上記ランダムパターン情報記録部から検出されるランダムパターン情報に基づいて生成された媒体識別情報を認証データとして格納した認証データ記録部とを有する情報記録媒体から情報を再生する情報再生装置であって、情報記録媒体上のランダムパターン情報記録部からランダムパターン情報を検出するランダムパターン情報検出部と、上記ランダムパターン情報検出部により検出されたランダムパターン情報から媒体識別情報検査データを生成する検査データ生成部と、情報記録媒体上の認証データ記録部から認証データを読み出し、上記検査データ生成部により生成された媒体識別情報検査データと上記認証データに基づいて情報記録媒体に対する認証処理を行う認証処理部と、情報を情報記録媒体から読み出す制御を行う再生制御部とを具備することを特徴とする。

また、本発明は、情報記録媒体に認証のための情報を記録する認証データ記録装置において、ランダムな物理現象によるランダムパターン情報が記録された情報記録媒体上のランダムパターン情報記録部から上記ランダムパターン情報を検出するランダムパターン情報検出部と、上記ランダムパターン情報検出部により検出された上記ランダムパターン情報から媒体識別情報を生成する媒体識別情報生成部と、上記媒体識別情報生成部により生成した媒体識別情報を認証データとして上記情報記録媒体上の認証データ記録部に記録す

る制御を行う認証データ記録制御部とを具備することを特徴とする。

また、本発明は、情報記録媒体に対する認証処理を行う認証処理装置において、情報記録媒体上のランダムパターン情報記録部からランダムパターン情報を検出するランダムパターン情報検出部と、上記ランダムパターン情報検出部により検出されたランダムパターン情報から媒体識別情報検査データを生成する検査データ生成部と、情報記録媒体上の認証データ記録部から認証データを再生し、上記検査データ生成部により生成された媒体識別情報検査データと上記認証データに基づいて情報記録媒体に対する認証処理を行う認証処理部とを具備することを特徴とする。

また、本発明は、情報を記録し、再生する情報記録再生方法であって、情報記録媒体上のランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部からランダムな物理現象によるランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報を生成して、上記媒体識別情報を認証データとして上記情報記録媒体上の認証データ記録部に記録する制御を行う認証データ記録制御工程と、上記ランダムパターン情報記録部から上記ランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報検査データを生成するとともに、上記情報記録媒体上の認証データ記録部から認証データを読み出し、上記ランダムパターン情報から生成した媒体識別情報検査データと上記認証データに基づいて上記情報記録媒体に対する認証処理を行う認証処理工程と、上記認証処理工程の認証結果に基づいて、情報記録媒体への情報記録及び情報記録媒体からの情報再生の制御を行う情報記録再生制御工程とを具備することを特徴とする。

また、本発明は、ランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部と、上記ランダムパターン情報記録部から検出されるランダムパターン情報に基づいて生成された媒体識別情報を認証データとして格納した認証データ記録部とを有する情報記録媒体に情報を記録する情報記録方法であって、情報記録媒体上のランダムパターン情報記録部からランダムパターン情報を検出するランダムパターン情報検出工程と、上記ランダムパターン情報検出工程により検出されたランダムパターン情報から媒体識別情報検査データを生成する検査データ生成工程と、情報記録媒体上の認証データ記録部から認証データを読み出し、上記検査データ生成工程により生成された媒体識別情報検査データと上記認証データに基づいて、情報記録媒体に対する認証処理を行い、認証結果に基づいて情報の情報記録媒体への書き込みの可否を制御する認証処理工程と、情報を情報記録媒体に記録する制御を行う記録制御工程と具備することを特徴とする。

また、本発明は、ランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部と、上記ランダムパターン情報記録部から検出されるランダムパターン情報に基づいて生成された媒体識別情報を認証データとして格納した認証データ記録部とを有する情報記録媒体から情報を再生する情報再生方法であって、情報記録媒体上のランダムパターン情報記録部からランダムパターン情報を検出するランダムパターン情報検出工程と、上記ランダムパターン情報検出工程により検出されたランダムパターン情報から媒体識別情報検査データを生成する検査データ生成工程と、情報記録媒体上の認証データ記録部から認証データを読み出し、上記検査



データ生成工程により生成された媒体識別情報検査データと上記認証データに基づいて情報記録媒体に対する認証処理を行う認証処理工程と、情報を情報記録媒体から読み出す制御を行う再生制御工程とを具備することを特徴とする。

また、本発明は、情報記録媒体に認証のための情報を記録する認証データ記録方法において、ランダムな物理現象によるランダムパターン情報が記録された情報記録媒体上のランダムパターン情報記録部から上記ランダムパターン情報を検出するランダムパターン情報検出工程と、上記ランダムパターン情報検出工程により検出された上記ランダムパターン情報から媒体識別情報を生成する媒体識別情報生成工程と、上記媒体識別情報生成工程により生成した媒体識別情報を認証データとして上記情報記録媒体上の認証データ記録部に記録する制御を行う認証データ記録制御工程とを具備することを特徴とする。

また、本発明は、情報記録媒体に対する認証処理を行う認証処理方法において、情報記録媒体上のランダムパターン情報記録部からランダムパターン情報を検出するランダムパターン情報検出工程と、上記ランダムパターン情報検出工程により検出されたランダムパターン情報から媒体識別情報検査データを生成する検査データ生成工程と、情報記録媒体上の認証データ記録部から認証データを再生し、上記検査データ生成工程により生成された媒体識別情報検査データと上記認証データに基づいて情報記録媒体に対する認証処理を行う認証処理工程とを具備することを特徴とする。

また、本発明は、情報が記録される情報記録媒体において、ランダムな物理現象によるランダムパターン情報が記録されたランダム

パターン情報記録部と、上記ランダムパターン情報記録部から検出されるランダムパターン情報に基づいて生成された媒体識別情報が認証データとして記録された認証データ記録部と、情報が記録される情報記録部とを具備することを特徴とする。

#### 図面の簡単な説明

図 1 は、本発明を適用した光ディスクを説明するための図である。

図 2 は、上記光ディスクに認証データを記録する認証データ記録装置の構成を示すブロック図である。

図 3 は、上記認証データ記録装置における認証データ生成部の具体的な処理内容を示すフローチャートである。

図 4 は、上記光ディスクを使用する光ディスク記録／再生装置の構成を示すブロック図である。

図 5 は、上記光ディスク記録／再生装置における認証処理部の具体的な処理内容を示すフローチャートである。

図 6 は、上記認証処理部による認証処理に使用されるリボケーションリストを示す図である。

図 7 は、上記認証処理部による認証処理に使用される公開鍵リストを示す図である。

図 8 は、上記光ディスク記録／再生装置における記録／再生回路の暗号化処理部の構成を示すブロック図である。

図 9 は、上記光ディスク記録／再生装置により光ディスクに記録されるデータの構造を模式的に示す図である。

図 10 は、上記光ディスク記録／再生装置における記録／再生回

路の復号処理部の構成を示すブロック図である。

図 1 1 は、上記光ディスク記録／再生装置の記録モードの動作を示すフローチャートである。

図 1 2 は、上記光ディスク記録／再生装置の再生モードの動作を示すフローチャートである。

図 1 3 は、上記光ディスク記録／再生装置における記録／再生回路の暗号化処理部の他の構成例を示すブロック図である。

図 1 4 は、上記光ディスク記録／再生装置における記録／再生回路の復号処理部の他の構成例を示すブロック図である。

図 1 5 は、本発明を適用したカード状情報記録媒体を説明するための図である。

#### 発明を実施するための最良の形態

以下、本発明を実施するための最良の形態について図面を参照しながら詳細に説明する。

本発明は、例えば図 1 に示すような構成の光ディスク 1 を用いた記録／再生システムに適用される。

図 1 に示した光ディスク 1 は、情報の記録／再生が可能なディスク媒体であり、中心孔 2 を中心としてそれぞれ環状に形成された 3 つの情報記録領域であるユーザデータ記録部 3、ランダムパターン情報記録部 4 及び認証データ記録部 5 を有する。上記ユーザデータ記録部 3、ランダムパターン情報記録部 4 及び認証データ記録部 5 は、それぞれ独立にアクセスして情報を読み出すことができるよう

に、例えば、2次元的に分離した状態、又は、3次元的に分離した状態に配置される。

この光ディスク1では、情報記録領域をディスク半径方向に2次元的に分離することにより、上記ユーザデータ記録部3、ランダムパターン情報記録部4及び認証データ記録部5が形成されている。

この光ディスク1において、外周側に形成されたユーザデータ記録部3は、ユーザデータが記録／再生されるデータエリアである。すなわち、映像若しくは音楽等のコンテンツが記録されるエリアである。

また、内周側に形成されたランダムパターン情報記録部4は、ランダムな物理現象によるランダムパターン情報が記録された読み取り専用の領域である。

このランダムパターン情報記録部4は、メディアの製造時に例えば磁気を帯びた細かい繊維を、このランダムパターン情報記録部4の領域にランダムに撒いて固定することにより形成される。このようにして形成されたランダムパターン情報記録部4は、上記磁気を帯びた細かい繊維によるランダムパターン情報が検出可能に記録されたものとなる。

なお、上記ランダムパターン情報記録部4は、ランダムにビットを形成し、そのジッターをランダムパターン情報として検出することができるようにしてもよい。

さらに、上記ランダムパターン情報記録部4の外周側に形成された認証データ記録部5は、上記ランダムパターン情報記録部4から検出されるランダムパターン情報に基づいて生成された媒体識別情報と、上記媒体識別情報に対する製造者毎のデジタル署名が認証デ

ータとして記録された領域である。この認証データ記録部 5 は、リードインエリアに設けられている。

このような構成の光ディスク 1 は、例えば図 2 に示すような構成の認証データ記録装置 10 により、上記認証データ記録部 5 に認証データが記録される。

この図 2 に示した認証データ記録装置 10 は、サーボ回路 11 により制御されるスピンドルモータ 12、上記光ディスク 1 の情報記録面を光学的に走査する記録／再生ヘッド 13、上記光ディスク 1 のランダムパターン情報記録部 4 からランダムパターン情報を検出するランダムパターン情報検出部 14、媒体識別情報 r を生成する媒体識別情報生成部 15、認証データを生成する認証データ生成部 16、入力操作部 17 から入力される設定情報に基づいて上記サーボ回路 11 や認証データ生成部 16 を制御する制御部 18 等を備える。

上記スピンドルモータ 12 は、サーボ回路 11 による制御に基づいて、上記光ディスク 1 を例えば線速度一定の状態 で回転駆動させる。

上記記録／再生ヘッド 13 は、上記スピンドルモータ 12 により回転駆動される光ディスク 1 の認証データ記録部 5 を光学的に走査する光学ヘッドからなり、上記認証データ記録部 5 を介して認証データの記録／再生を行う。

上記ランダムパターン情報検出部 14 は、上記スピンドルモータ 12 により回転駆動される光ディスク 1 のランダムパターン情報記録部 4 を走査する磁気ヘッドからなり、上記ランダムパターン情報記録部 4 からランダムパターン情報をアナログ的に検出する。この

ランダムパターン情報検出部 14 は、上記ランダムパターン情報記録部 4 から検出したランダムパターン情報を上記媒体識別情報生成部 15 に供給する。

上記媒体識別情報生成部 15 は、上記ランダムパターン情報検出部 14 によりアナログ的に検出されたランダムパターン情報からデジタルのランダムパターン情報に変換し、これを媒体識別情報  $r$  として上記認証データ生成部 16 に供給する。

上記認証データ生成部 16 は、上記媒体識別情報生成部 15 から供給される媒体識別情報  $r$  に該媒体識別情報  $r$  に対する製造者毎のデジタル署名を付して認証データとする。

ここで、上記認証データ生成部 16 により製造者毎のデジタル署名を付した認証データを生成するに当たり、記録媒体の製造者は、信頼できるトラステッド・センター(TC:Trusted Center)を使用し、デジタル署名の検証に必要な自分の公開鍵をTCに登録し、証明書(Cert)を発行してもらっておく。証明書(Cert)は、製造者の識別情報IDや公開鍵などにTCがデジタル署名を施したデータである。

また、デジタル署名技術は、データを生成したのが特定のユーザであることを証明できる技術であり、例えばIEEE P1363で使用されているElliptic Curve Digital Signature Algorithm(ECDSA)方式などがよく知られている。

この認証データ記録装置 10 では、上記認証データ生成部 16 の具体的な処理内容を図3に示してあるように、上記媒体識別情報生成部 15 から供給される媒体識別情報  $r$  に媒体製造日や製造者の識別情報IDなどの付加情報  $u$  を付加して、データ  $m$  を生成する(ステップ S1)。このデータ  $m$  に対し、トラステッド・センターに登録

した公開鍵に対応する製造者別の秘密鍵を用いてデジタル署名データ  $s$  を生成する（ステップ  $S2$ ）。

なお、上記付加情報  $u$  は、必要に応じて上記媒体識別情報  $r$  に付加すればよいデータである。

そして、上記認証データ生成部 16 は、上記データ  $m$  とデジタル署名データ  $s$  と証明書 (Cert) データをリボケーションリストを合わせて認証データ  $w$  とし（ステップ  $S3$ ）、この認証データ  $w$  を上記記録／再生ヘッド 13 に供給する（ステップ  $S4$ ）ことにより、上記光ディスク 1 の認証データ記録部 5 に記録する。

ここで、上記付加情報  $u$ 、製造者別の秘密鍵及び証明書 (Cert) データは、例えば上記入力操作部 17 から上記制御部 18 に入力されることにより、上記制御部 18 から上記認証データ生成部 16 に与えられる。

この認証データ記録装置 10 では、トラステッド・センターから与えられるリボケーションリストを上記入力操作部 17 から上記制御部 18 に入力することにより、上記リボケーションリストを上記制御部 18 から上記認証データ生成部 16 に与えて、上記光ディスク 1 の認証データ記録部 5 に記録することができるようになっている。上記光ディスク 1 の認証データ記録部 5 には、トラステッド・センターから与えられる最新版のリボケーションリストを記録する。

ここで、リボケーションリストは、単調増加であるそのバージョンナンバーと、秘密鍵が露呈したり不正を働いたと判断された製造者の識別情報  $ID$  にトラステッド・センターがデジタル署名を施したものである。

記録媒体の製造者は、このような構成の認証データ記録装置 10

により、上記データ  $m$  とデジタル署名データ  $s$  と証明書 (Cert) データとリボケーションリストを認証データ  $w$  として認証データ記録部 5 に記録した光ディスク 1 を製造することができる。

このような構成の光ディスク 1 は、ランダムな物理現象によるランダムパターン情報が記録されたランダムパターン情報記録部 4 から検出されるランダムパターン情報と、認証データ記録部 16 に記録されている認証データによる認証処理により正当性を検証することができる。上記ランダムパターン情報記録部 4 に記録されているランダムパターン情報は、ランダムな物理現象によるものであるから、複製することはできない。

上述の如き構成の光ディスク 1 は、例えば図 4 に示すような構成の光ディスク記録／再生装置 20 により、データの記録／再生が行われる。

図 4 に示した光ディスク記録／再生装置 20 は、サーボ回路 21 により制御されるスピンドルモータ 22、上記光ディスク 1 の情報記録面を光学的に走査する記録／再生ヘッド 23、上記光ディスク 1 のランダムパターン情報記録部 4 からランダムパターン情報を検出するランダムパターン情報検出部 24、媒体識別情報検査データ  $r'$  を生成する媒体識別情報検査データ生成部 25、認証処理部 26、記録／再生部 27、入力操作部 28 から入力される設定情報に基づいて上記サーボ回路 21 や記録／再生部 27 を制御する制御部 19 等を備える。

上記スピンドルモータ 22 は、サーボ回路 21 による制御に基づいて、上記光ディスク 1 を例えば線速度一定の状態で回転駆動させる。



上記記録／再生ヘッド 23 は、上記スピンドルモータ 22 により回転駆動される光ディスク 1 の情報記録面を認証データ記録部 5 を光学的に走査する光学ヘッドからなり、上記認証データ記録部 5 に記録されている認証データの再生や、上記ユーザデータ部 3 に対するデータの記録／再生を行う。

上記ランダムパターン情報検出部 24 は、上記スピンドルモータ 22 により回転駆動される光ディスク 1 のランダムパターン情報記録部 4 を走査する磁気ヘッドからなり、上記ランダムパターン情報記録部 4 からランダムパターン情報をアナログ的に検出する。このランダムパターン情報検出部 24 は、上記ランダムパターン情報記録部 4 から検出したランダムパターン情報を上記媒体識別情報検査データ生成部 25 に供給する。

上記媒体識別情報検査データ生成部 25 は、上記ランダムパターン情報検出部 24 によりアナログ的に検出されたランダムパターン情報からデジタルのランダムパターン情報に変換し、これを媒体識別情報検査データ  $r'$  として上記認証処理部 26 に供給する。

上記認証処理部 26 は、上記光ディスク 1 が正当な製造者により製造されたものであることを認証する処理を行うものである。この認証処理部 26 は、上記記録／再生ヘッド 23 により上記光ディスク 1 の認証データ記録部 5 から再生される認証データ  $w^{\wedge}$  が記録／再生部 27 を介して供給されており、上記媒体識別情報生成部 25 から供給される媒体識別情報検査データ  $r'$  と上記認証データ  $w^{\wedge}$  に基づいて認証処理を行う。

上記認証処理部 26 の具体的な処理内容を図 5 に示してある。

すなわち、上記認証処理部 26 は、上記媒体識別情報検査データ

$r'$  と上記認証データ  $w^{\wedge}$  を取り込むと（ステップ S 1 1）、先ず、上記認証データ  $w^{\wedge}$  に入っているリボケーションリストの正当性すなわちトラステッド・センターのデジタル署名の正当性をトラステッド・センターの公開鍵を用いて検証する（ステップ S 1 2）。トラステッド・センターの公開鍵は、システム全体で共通であり、機器を製造する際に機器内の不揮発性メモリに格納されている。

上記リボケーションリストの検証の結果、リボケーションリストが正当なものであったら、上記リボケーションリストのバージョンナンバーを検証し（ステップ S 1 3）、現在保存しているリボケーションリストと比較しバージョンナンバーが新しい場合には、不揮発性メモリに格納する（ステップ S 1 4）。不揮発性メモリは、図 6 に示すようなリボケーションリストが格納される。

次に、上記認証データ  $w^{\wedge}$  中の証明書 (Cert) データを取り出し（ステップ S 1 5）、上記証明書 (Cert) データに含まれる製造者の識別情報 ID が上記不揮発性メモリに格納しているリボケーションリストに載っていないことを検証し（ステップ S 1 6）、さらに、上記証明書 (Cert) データに含まれるトラステッド・センターのデジタル署名が正しいことを検証する（ステップ S 1 7）。

この検証に合格したら、上記認証データ  $w^{\wedge}$  からデータ  $m^{\wedge}$  とデジタル署名データ  $s^{\wedge}$  を取り出し（ステップ S 1 8）、上記認証データ  $w^{\wedge}$  中のデジタル署名データ  $s^{\wedge}$  がデータ  $m^{\wedge}$  に対する製造者の正しいデジタル署名になっていることを、上記証明書 (Cert) データ中の製造者の公開鍵を用いて検証する（ステップ S 1 9）。

上記検証に合格したら、検証結果 J 2 を合格とする（ステップ S 2 0）。

次に、上記認証データ  $w^{\wedge}$  から媒体識別情報  $r^{\wedge}$  と付加情報  $u^{\wedge}$  を取り出す（ステップ S 2 1）。

そして、上記認証データ  $w^{\wedge}$  から取り出した媒体識別情報  $r^{\wedge}$  と上記媒体識別情報生成部 2 5 により生成された媒体識別情報検査データ  $r'$  とを比較し、予め定められた誤差内に収まっていることを検証する（ステップ S 2 2）。ここでは、アナログ信号として検出されたランダムパターン情報からデジタルの媒体識別情報検査データ  $r'$  を生成しているため、多少のノイズにより誤差を含む可能性があるため、許容誤差範囲を設けている。ランダムパターン情報をディジタルで記録し、読み出せるように構成している場合には、この許容誤差範囲を設定しなくてもかまわない。

この検証に合格したら、検証結果 J 1 を合格とする（ステップ S 2 3）。

上記検証結果 J 1 と検証結果 J 2 が共に合格となれば、この記録媒体を正当なものと判断し、上記媒体識別情報  $r^{\wedge}$  を認証済みの媒体識別情報 DiscID として記録／再生部 2 7 に供給する（ステップ S 2 4）。

ここで、上記不揮発性メモリは、図 7 に示すような公開鍵リストを格納するようにすることもできる。

この場合、公開鍵リストには、製造者の識別情報 ID と、その公開鍵、識別情報 ID がリボークされているか否かを示すフラグが格納される。さらに、その機器が扱ったことのあるリボケーションリストのうち最新のバージョンのもののバージョンナンバーが格納される。

この機器がデータ  $w^{\wedge}$  から、機器が扱ったいずれのものより新し

い、正当なりボケーションリストを得た場合、そのリストに挙げられている識別情報 I D に対応するなりボケーションフラグを Y E S すなわちリボークとする。

もしそれまでその識別情報 I D がテーブル上になければ、その項目を新規に作成してフラグを Y E S とする。

逆に、機器が格納していたテーブルにはあったが、最新のなりボケーションリストに識別情報 I D が含まれていないものについては、フラグをすべて N O、すなわちリボークしないとする。そして、最新のバージョンナンバーの項目を更新する。

上記認証データ w ^ 中から取り出した証明書 (Cert) データを検証する際には、製造者の識別情報 I D をチェックし、その識別情報 I D の項目が格納してあるリストにあり、その公開鍵が記録されていて、なりボケーションフラグが N O であれば、証明書 (Cert) データの検証は不要であり、テーブルに記録されている公開鍵を使用する。

識別情報 I D の項目がテーブルにあり、フラグが N O であり、公開鍵が記録されていない場合には、証明書 (Cert) データを検証して、正しい場合に公開鍵をテーブルに格納する。

識別情報 I D の項目がテーブルにあり、フラグが Y E S である場合には、検証 J 2 の結果を不合格とする。

識別情報 I D の項目がテーブルにない場合には、証明書 (Cert) データを検証して、正しい場合に、その識別情報 I D に対応する項目を新規に作成して公開鍵を格納する。このときフラグは N O とする。

このように公開鍵リストを持つことにより、多くの場合、すなわち、同一の製造者が製造した媒体を使用するが 2 回目以降になる場合のほとんどで証明書 (Cert) データの検証を省くことが可能となる。

この光ディスク記録／再生装置 20 において、上記記録／再生部 27 は、入力操作部 28 から入力される制御命令に応じて制御部 29 により動作モードが切り換えられる。この記録／再生部 27 は、暗号化処理部 30 と復号処理部 40 を備えており、記録モードには、外部から入力されるユーザデータを上記暗号化処理部 30 により暗号化し、暗号化したユーザデータを上記記録／再生ヘッド 23 を介して上記光ディスク 1 のユーザデータ部 3 に記録し、また、再生モード時には、上記記録／再生ヘッド 23 により上記光ディスク 1 のユーザデータ部 3 から再生される暗号化されたユーザデータを復号処理部 40 により復号して外部に出力するようになっている。

上記暗号化処理部 30 は、その具体的な構成を図 8 に示すように、K e m 発生モジュール 31、乱数発生回路 32、K d 暗号化／復号回路 33、K s 暗号化回路 34 やコンテンツデータ暗号化回路 35 等からなる。

上記 K e m 発生モジュール 31 は、マスターキー K m を記憶した K m メモリ 31 A と、上記 K m メモリ 31 A から上記マスターキー K m が与えられるとともに上記認証処理部 26 から認証済みの媒体識別情報 DiscID が供給されるハッシュ関数回路 31 B とからなる。

上記マスターキー K m は、著作権のライセンスを受ける際に与えられる秘密鍵である。

上記ハッシュ関数回路 31 B は、n ビットのマスターキー K m と m ビットの媒体識別情報 DiscID とを連結して、例えば下位ビットをマスターキー K m とし上位ビットを媒体識別情報 DiscID とした n + m ビットの連結データ (DiscID || K m) を生成し、生成した連結データ (DiscID || K m) に対して、次の (1) 式に示すように h a s h 関

数Hを適用して、

$$K_{em} = H(DiscID \parallel K_m) \quad (1)$$

イフェクティブマスターキー $K_{em}$ を生成する。そして、上記ハッシュ関数回路31Bは、上記マスターキー $K_m$ と認証済みの媒体識別情報DiscIDから生成したイフェクティブマスターキー $K_{em}$ を $K_d$ 暗号化／復号回路33に供給する。

ここで、 $A \parallel B$ の記号“ $\parallel$ ”は、データAとデータBの連結を意味する。また、hash関数は、任意長の入力データに対して、例えば64ビット又は128ビットなどの固定長のデータを出力する関数であり、 $y (= hash(x))$ を与えられたとき、 $x$ を求めることが困難であり、かつ、 $hash(x_1) = hash(x_2)$ となる $x_1$ と $x_2$ との組を求めることも困難となる関数である。一方向hash関数の代表的なものとしてMD(Message Digest)5やSHA(Secure Hash Algorithm)などが知られている。この一方向hash関数については、Bruce Schneier著「Applied Cryptography(Second Edition), Wiley」に詳しく解説されている。

また、上記乱数発生回路32は、セクタキー $K_{si}$ とディスクキー $K_d$ として用いる乱数を発生し、セクタキー $K_{si}$ を上記 $K_s$ 暗号化回路34とコンテンツデータ暗号化回路35に供給するとともに、ディスクキー $K_d$ を上記 $K_d$ 暗号化／復号回路33と $K_s$ 暗号化回路34に供給する。

上記 $K_d$ 暗号化／復号回路33は、上記乱数発生回路32から供給されるディスクキー $K_d$ を上記イフェクティブマスターキー $K_{em}$ で暗号化して暗号化ディスクキー $E K_d$ を生成する。この $K_d$ 暗号化／復号回路33により生成された暗号化ディスクキー $E K_d$ は、

上記記録／再生ヘッド 23 を介して上記光ディスク 1 のリードインエリアに記録される。また、この K d 暗号化／復号回路 33 は、上記記録／再生ヘッド 23 を介して上記光ディスク 1 のリードインエリアから再生される暗号化ディスクキー E K d を復号してディスクキー K d を生成する。この K d 暗号化／復号回路 33 により生成されたディスクキー K d は、上記 K s 暗号化回路 35 に供給される。

また、上記 K s 暗号化回路 34 は、上記乱数発生回路 32 から供給されるセクタキー K s i を上記ディスクキー K d で暗号化して暗号化セクタキー E K s を生成する。この K s 暗号化回路 34 により生成された暗号化セクタキー E K s は、上記記録／再生ヘッド 23 を介して上記光ディスク 1 のデータエリアに記録される。

さらに、上記コンテンツデータ暗号化回路 35 は、外部からコンテンツデータとして供給されるユーザデータを上記セクタキー K s i で暗号化することにより、暗号化コンテンツデータを生成する。

この上記コンテンツデータ暗号化回路 35 により生成された暗号化コンテンツデータは、上記記録／再生ヘッド 23 を介して上記光ディスク 1 のデータエリアに記録される。

ここで、上記光ディスク 1 のデータエリアは、図 9 に示すように、複数のセクタ S i ( i = 1, 2, . . . ) からなる。各セクタ S i ( i = 1, 2, . . . ) は、ヘッダ及びメインデータ部で構成されており、上記セクタキー K s i をディスクキー K d で暗号化した暗号化セクタキー E K s i ( i = 1, 2, . . . ) が各セクタ S i のヘッダに格納され、ユーザデータを上記セクタキー K s i で暗号化した暗号化コンテンツデータが各セクタ S i のメインデータ部に格納される。上記 i = 1, 2, . . . はセクタの番号を示している。

なお、簡略化のため、一部の図及び説明文中では、セクタ番号を省略する。

また、上記復号処理部40は、その具体的な構成を図10に示すように、K<sub>e</sub>m発生モジュール41、E<sub>K</sub>d復号回路43、E<sub>K</sub>s復号回路44やコンテンツデータ復号回路45等からなる。

上記K<sub>e</sub>m発生モジュール41は、著作権のライセンスを受ける際に与えられる秘密鍵であるマスターキーK<sub>m</sub>を記憶したK<sub>m</sub>メモリ41Aと、上記K<sub>m</sub>メモリ41Aにより与えられるマスターキーK<sub>m</sub>と上記認証処理部26により与えられる認証済みの媒体識別情報DiscIDから上述の(1)式に示した演算処理によりイフェクティブマスターキーK<sub>e</sub>mを生成するハッシュ関数回路41Bとからなる。上記ハッシュ関数回路41Bは、上記マスターキーK<sub>m</sub>と認証済みの媒体識別情報DiscIDから生成したイフェクティブマスターキーK<sub>e</sub>mをE<sub>K</sub>d復号回路43に供給する。

なお、このK<sub>e</sub>m発生モジュール41は、上述の暗号化処理部30のK<sub>e</sub>m発生モジュール31と同じ構成のものであり、上記K<sub>e</sub>m発生モジュール31を兼用するようにしてもよい。

上記E<sub>K</sub>d復号回路43は、上記光ディスク1のリードインエリアから上記記録／再生ヘッド23により再生される暗号化ディスクキーE<sub>K</sub>dを上記イフェクティブマスターキーK<sub>m</sub>で復号してディスクキーK<sub>d</sub>を生成し、復号したディスクキーK<sub>d</sub>をE<sub>K</sub>s復号回路44に供給する。

また、上記E<sub>K</sub>s復号回路44は、上記光ディスク1のデータエリアから上記記録／再生ヘッド23により再生される暗号化セクタキーE<sub>K</sub>sを上記ディスクキーK<sub>d</sub>で復号してセクタキーK<sub>s</sub>を生



成し、復号したセクタキー $K_s$ をコンテンツデータ復号回路45に供給する。

上記コンテンツデータ復号回路45は、上記光ディスク1のデータエリアから上記記録／再生ヘッド23により再生される暗号化コンテンツデータを上記セクタキー $K_s$ で復号する。

このような構成の光ディスク記録／再生装置20では、上記入力操作部28から記録命令が入力されることにより制御部29に記録モードが設定されると、上記制御部29は、図11のフローチャートに示すような手順でユーザデータを光ディスク1に記録するように、上記記録／再生部27を制御する。

なお、以下の説明では、上記認証処理部26により光ディスク1に対して既に認証処理が行われており、正当なものであると認証された光ディスク1に対してユーザデータを記録するものとする。

記録モードでは、上記記録／再生部27の暗号化処理部30が動作状態となっており、上記暗号化処理部30の $K_{em}$ 発生モジュール31は、上記認証処理部26から認証済みの媒体識別情報DiscIDを受け取り（ステップS31）、マスターキー $K_m$ を $K_m$ メモリ31Aから読み出して（ステップS32）、ハッシュ関数回路31Bにより上記媒体識別情報DiscIDとマスターキー $K_m$ からイフェクティブマスターキー $K_{em}$ を生成する（ステップS33）。

次に、上記 $K_d$ 暗号化／復号回路33は、上記光ディスク1のリードインエリアに暗号化ディスクキー $E_{K_d}$ が記録されているか否かを判定する（ステップS34）。

そして、上記 $K_d$ 暗号化／復号回路33は、暗号化ディスクキー $E_{K_d}$ が記録されていない場合には、乱数発生回路32により発生

される例えば40ビットの乱数をディスクキーK<sub>d</sub>とし（ステップS35）、このディスクキーK<sub>d</sub>を上記イフェクティブマスターキーK<sub>em</sub>で暗号化して暗号化ディスクキーEK<sub>d</sub>を生成し、この暗号化ディスクキーEK<sub>d</sub>を上記光ディスク1のリードインエリアに記録する（ステップS36）。

また、上記K<sub>d</sub>暗号化／復号回路33は、暗号化ディスクキーEK<sub>d</sub>が記録されていた場合には、上記暗号化ディスクキーEK<sub>d</sub>を上記イフェクティブマスターキーK<sub>m</sub>で復号して、ディスクキーK<sub>d</sub>を得る（ステップS37）。

次に、上記K<sub>s</sub>暗号化回路34は、上記乱数発生回路32により発生される40ビットの乱数をセクタキーK<sub>si</sub>とし（ステップS38）、このセクタキーK<sub>si</sub>を上記ディスクキーK<sub>d</sub>で暗号化して暗号化セクタキーEK<sub>si</sub>を生成し、この暗号化セクタキーEK<sub>si</sub>をセクタヘッドに記録する（ステップS39）。

そして、上記コンテンツデータ暗号化回路35は、ユーザデータを上記セクタキーK<sub>si</sub>で暗号化して暗号化コンテンツデータを生成し、この暗号化コンテンツデータは、メインデータ部に記録する（ステップS40）。

さらに、上記コンテンツデータ暗号化回路35は、記録すべきユーザデータをすべて記録したか否かを判定し（ステップS41）、記録すべきユーザデータがある場合には、次のセクタにアクセスし（ステップS42）、上記ステップS38に戻って、上記ステップS38からステップS42の処理を繰り返す。

このようにしてユーザデータをすべて上記光ディスク1のデータエリアに記録し終えたら、記録モードを終了する。

また、この光ディスク記録／再生装置 20 では、上記入力操作部 28 から記録命令が入力されることにより制御部 29 に再生モードが設定されると、上記制御部 29 は、図 12 のフローチャートに示すような手順で光ディスク 1 からユーザデータを再生するように、上記記録／再生部 27 を制御する。

なお、以下の説明では、上記認証処理部 26 により光ディスク 1 に対して既に認証処理が行われており、正当なものであると認証された光ディスク 1 からユーザデータを再生するものとする。

再生モードでは、上記記録／再生部 27 の復号処理部 40 が動作状態となっており、上記復号処理部 40 の K e m 発生モジュール 41 は、上記認証処理部 26 から認証済みの媒体識別情報 DiscID を受け取り（ステップ S 5 1）、マスターキー K m を K m メモリ 41 A から読み出して（ステップ S 5 2）、ハッシュ関数回路 41 B により上記媒体識別情報 DiscID とマスターキー K m からイフェクティブマスターキー K e m を生成する（ステップ S 5 3）。

次に、上記 E K d 復号回路 43 は、上記光ディスク 1 のリードインエリアから再生される暗号化ディスクキー E K d を上記イフェクティブマスターキー K e m で復号して、ディスクキー K d を生成する（ステップ S 5 4）。

次に、上記 E K s 復号回路 44 は、上記光ディスク 1 のデータエリアから再生される暗号化セクタキー E K s i を復号して、セクタキー K s i を生成する（ステップ S 5 5）。

そして、上記コンテンツデータ復号回路 45 は、上記光ディスク 1 のデータエリアから再生される暗号化コンテンツデータを上記セクタキー K s で復号する（ステップ S 5 6）。

さらに、上記コンテンツデータ復号回路45は、再生すべきコンテンツデータをすべて再生したか否かを判定し（ステップS57）、再生すべきコンテンツデータがある場合には、次のセクタにアクセスし（ステップS58）、上記ステップS25に戻って、上記ステップS55からステップS58の処理を繰り返し行う。

このようにして必要なコンテンツデータをすべて上記光ディスク1のデータエリアから再生し終えたら、再生モードを終了する。

この光ディスク記録／再生装置20によりユーザデータ記録部3にユーザデータが記録された光ディスク1は、上記ユーザデータの暗号鍵すなわちセクタキーK<sub>s</sub>が上記ディスクキーK<sub>d</sub>で暗号化した暗号化セクタキーEK<sub>s</sub>としてデータエリアに記録され、さらに、上記ディスクキーK<sub>d</sub>が、この光ディスク1に固有の媒体識別情報DiscIDとマスターキーK<sub>m</sub>とに基づいて生成されたイフェクティブマスターキーK<sub>em</sub>で暗号化した暗号化ディスクキーEK<sub>d</sub>としてリードインエリアに記録されているので、上記光ディスク1のランダムパターン情報記録部4に記録されているランダムパターン情報に基づいて生成される媒体識別情報検査データと認証データ記録部5に記録された認証データに基づいて上記媒体識別情報DiscIDについて認証処理を行う認証処理機能及びマスターキーK<sub>m</sub>を有する正規の再生装置でのみ再生することができ、上記認証処理機能若しくはマスターキーK<sub>m</sub>を持たない再生装置ではユーザデータを復号して再生することはできない。

また、仮に、上記光ディスク1のデータエリア及びリードインエリアのデータをそのまま新しいディスクに不正コピーされた場合としても、上記光ディスク1のランダムパターン情報記録部4に記録

されているランダムパターン情報はランダムな物理現象によるものであるから、上記新しいディスクがランダムパターン情報記録部を有する正規のものであったとしても、新しいディスクのランダムパターン情報記録部から上記光ディスク 1 のランダムパターン情報記録部 4 に記録されているランダムパターン情報と同じランダムパターン情報を検出することはできない。したがって、不正コピーされたディスクが正規の再生装置により再生されることはない。

ここで、上述の光ディスク記録／再生装置 20 では、暗号化処理処理部 30 において、上記認証処理部 26 により認証された光ディスク 1 の媒体識別情報 Disc I D に基づいて、マスターキー  $K_m$  からイフェクティブマスターキー  $K_{em}$  を生成し、このイフェクティブマスターキー  $K_{em}$  でディスクキー  $K_d$  を暗号化し、上記ユーザデータの暗号化に用いる暗号鍵すなわちセクターキー  $K_s$  を上記ディスクキー  $K_d$  で暗号化し、上記セクターキー  $K_s$  により暗号化したユーザデータと上記暗号化したディスクキー  $K_d$  及びセクターキー  $K_s$  を上記光ディスク 1 に記録するようにしたが、上記認証処理部 26 により認証された光ディスク 1 の媒体識別情報 Disc I D に基づいて、上記ユーザデータを暗号化するようにしてもよい。例えば、図 13 に示すように、上記乱数発生回路 32 で乱数として発生されるセクターキー  $K_s$  から上記イフェクティブマスターキー  $K_{em}$  に基づいてイフェクティブセクターキー  $K_{es}$  を生成するイフェクティブセクターキー生成回路 ( $K_{es}$  生成回路) 130 を設け、上記コンテンツデータ暗号化回路 35 において、上記イフェクティブセクターキー生成回路 130 により生成されたイフェクティブセクターキー  $K_{es}$  でユーザデータを暗号化して暗号化コンテンツデータ

を生成する。

この場合、復号処理部40には、図14に示すように、イフェクティブマスターキーK<sub>em</sub>に基づいてセクタキーK<sub>s</sub>からイフェクティブセクターキーK<sub>es</sub>を生成するイフェクティブセクターキー生成回路(K<sub>es</sub>生成回路)140を設け、上記光ディスク1のデータエリアから上記記録／再生ヘッド23により再生される暗号化セクタキーE<sub>Ks</sub>を上記E<sub>Ks</sub>復号回路44により上記ディスクキーK<sub>d</sub>で復号してセクターキーK<sub>s</sub>を生成し、このセクターキーK<sub>s</sub>から上記イフェクティブセクターキー生成回路140によりイフェクティブセクタキーK<sub>es</sub>を生成して、このイフェクティブセクタキーK<sub>es</sub>を用いてコンテンツデータ復号回路45により暗号化コンテンツデータを復号する。

また、上述の実施の形態では、図1に示すような構成の光ディスク1を用いた記録／再生システムに本発明を適用したが、図15に示すようなカード状記録媒体51を用いた記録／再生システムを構築するようにしてもよい。

すなわち、この図13に示したカード状記録媒体51は、ユーザデータが記録されるユーザデータ記録部53と、ランダムな物理現象によるランダムパターン情報が記録されたランダムパターン情報記録部54と、上記ランダムパターン情報記録部54から検出されるランダムパターン情報に基づいて生成された媒体識別情報と、上記媒体識別情報に対する製造者毎のデジタル署名が認証データとして記録された認証データ記録部55とを有する。

このような構成のカード状記録媒体51を使用する記録／再生システムでは、上述の光ディスク記録／再生システムと同様に、上記

ランダムパターン情報記録部 54 からランダムな物理現象によるランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報を生成するとともに、上記情報記録媒体上の認証データ記録部 55 から認証データを再生し、上記ランダムパターン情報から生成した媒体識別情報と上記認証データに基づいて上記情報記録媒体に対する認証処理を行うことができ、上記認証処理により認証された情報記録媒体の媒体識別情報から暗号鍵を生成し、上記暗号鍵を用いてデータを暗号化したデータを上記認証された情報記録媒体上のユーザデータ記録部 53 を介して記録／再生することにより、上記ユーザデータ記録部 53 の情報の不正コピーを確実に防止することが可能となる。

以上詳細に説明したように、本実施の形態によれば、情報記録媒体上にランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部を設けた情報記録媒体の上記ランダムパターン情報記録部からランダムな物理現象によるランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報を生成して、上記媒体識別情報を該媒体識別情報に対する製造者毎のデジタル署名とともに認証データとして上記情報記録媒体上の認証データ記録部に記録することによって、媒体識別情報を該媒体識別情報に対する製造者毎のデジタル署名とともに認証データとして認証データ記録部に記録した情報記録媒体を提供することができる。そして、ランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部と、上記ランダムパターン情報記録部から検出されるランダムパターン情報に基づいて生成された媒体識別情報と、上記媒体識別情報に対する製造者毎のデジタル署名を認証

データとして格納した認証データ記録部と、ユーザデータが記録されるユーザデータ記録部とを有する情報記録媒体に対して、上記ランダムパターン情報記録部からランダムな物理現象によるランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報を生成するとともに、上記情報記録媒体上の認証データ記録部から認証データを再生し、上記ランダムパターン情報から生成した媒体識別情報と上記認証データに基づいて上記情報記録媒体に対する認証処理を行うことができ、上記認証処理により認証された情報記録媒体の媒体識別情報から暗号鍵を生成し、上記暗号鍵を用いてデータを暗号化したデータを上記認証された情報記録媒体上のユーザデータ記録部を介して記録／再生することにより、記録可能媒体に対しても有効な不正コピー防止システムを構築することができる。



### 請求の範囲

#### 1. 情報を記録し、再生する情報記録再生システムであって、

情報記録媒体上のランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部からランダムな物理現象によるランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報を生成して、上記媒体識別情報を認証データとして上記情報記録媒体上の認証データ記録部に記録する制御を行う認証データ記録制御部と、

上記ランダムパターン情報記録部から上記ランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報検査データを生成するとともに、上記情報記録媒体上の認証データ記録部から認証データを読み出し、上記ランダムパターン情報から生成した媒体識別情報検査データと上記認証データに基づいて上記情報記録媒体に対する認証処理を行う認証処理部と、

上記認証処理部の認証結果に基づいて、情報記録媒体への情報記録及び情報記録媒体からの情報再生の制御を行う情報記録再生制御部と

を具備することを特徴とする情報記録再生システム。

#### 2. 上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、情報の暗号化の処理を行う暗号処理部を更に具備し、

上記情報記録再生制御部は、上記暗号処理部で暗号化された情報を、上記認証された情報記録媒体に記録する制御を行うことを特徴とする請求の範囲第1項記載の情報記録再生システム。

3. 上記情報記録再生制御部は、暗号化した情報と前記情報の暗号化に用いた暗号鍵とを上記認証された情報記録媒体に記録する制御を行うことを特徴とする請求の範囲第2項記載の情報記録再生システム。

4. 上記暗号処理部は、上記暗号化鍵を用いて情報を暗号化するとともに、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、上記情報の暗号化に用いた暗号鍵を暗号化し、

上記情報記録再生制御部は、上記暗号鍵により暗号化された情報と上記暗号化された暗号鍵とを上記認証された情報記録媒体に記録する制御を行うことを特徴とする請求の範囲第3項記載の情報記録再生システム。

5. 上記暗号処理部は、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、上記情報の暗号化に用いる暗号鍵を生成することを特徴とする請求の範囲第2項記載の情報記録再生システム。

6. 上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、情報の復号の処理を行う復号処理部を更に具備し、

上記情報記録再生制御部は、暗号化された情報を、上記認証された情報記録媒体から読み出す制御を行い、

上記復号処理部は、上記情報記録再生制御部によって情報記録媒体から読み出された暗号化された情報を、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、復号する処理を行うことを特徴とする請求の範囲第1項記載の情報記録再生システム。

7. 上記情報記録再生制御部は、暗号化された情報と前記情報の暗号化に用いた暗号鍵とを上記認証された情報記録媒体から読み出

す制御を行うことを特徴とする請求の範囲第 6 項記載の情報記録再生システム。

8. 上記情報記録再生制御部は、暗号化された情報と暗号化された前記暗号鍵とを上記認証された情報記録媒体から読み出す制御を行い、

上記復号処理部は、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、読み出された暗号化された暗号化鍵を復号するとともに、上記暗号化され情報を復号された暗号化鍵を用いて暗号化された情報を復号する処理を行うことを特徴とする請求の範囲第 7 項記載の情報記録再生システム。

9. 上記認証データ記録制御部は、上記媒体識別情報を該媒体識別情報の記録者のデジタル署名とともに認証データとして上記情報記録媒体上の認証データ記録部に記録することを特徴とする請求の範囲第 1 項記載の情報記録再生システム。

10. 上記認証データ記録制御部は、上記媒体識別情報の記録者のデジタル署名として、上記情報記録媒体の製造者のデジタル署名を記録することを特徴とする請求の範囲第 9 項記載の情報記録再生システム。

11. ランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部と、上記ランダムパターン情報記録部から検出されるランダムパターン情報に基づいて生成された媒体識別情報を認証データとして格納した認証データ記録部とを有する情報記録媒体に情報を記録する情報記録装置であって、

情報記録媒体上のランダムパターン情報記録部からランダムパターン情報を検出するランダムパターン情報検出部と、

上記ランダムパターン情報検出部により検出されたランダムパターン情報から媒体識別情報検査データを生成する検査データ生成部と、

情報記録媒体上の認証データ記録部から認証データを読み出し、上記検査データ生成部により生成された媒体識別情報検査データと上記認証データに基づいて、情報記録媒体に対する認証処理を行い、認証結果に基づいて情報の情報記録媒体への書き込みの可否を制御する認証処理部と、

情報を情報記録媒体に記録する制御を行う記録制御部とを具備することを特徴とする情報記録装置。

1 2. 上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、情報の暗号化の処理を行う暗号処理部を更に具備し、

上記記録制御部は、上記暗号処理部で暗号化された情報を、上記認証された情報記録媒体に記録する制御を行うことを特徴とする請求の範囲第 1 1 項記載の情報記録装置。

1 3. 上記記録制御部は、暗号化した情報と前記情報の暗号化に用いた暗号鍵とを上記認証された情報記録媒体に記録する制御を行うことを特徴とする請求の範囲第 1 2 項記載の情報記録装置。

1 4. 上記暗号処理部は、上記暗号化鍵を用いて情報を暗号化するとともに、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、上記情報の暗号化に用いた暗号鍵を暗号化し、

上記記録制御部は、上記暗号鍵により暗号化された情報と上記暗号化された暗号鍵とを上記認証された情報記録媒体に記録する制御を行うことを特徴とする請求の範囲第 1 3 項記載の情報記録装置。

1 5. 上記暗号処理部は、上記認証処理により認証された情報記

録媒体の媒体識別情報を用いて、上記情報の暗号化に用いる暗号鍵を生成することを特徴とする請求の範囲第 12 項記載の情報記録装置。

16. 上記認証処理部は、上記媒体識別情報が該媒体識別情報を記録した記録者のデジタル署名とともに認証データとして記録された情報記録媒体に対し、上記記録者のデジタル署名に基づいて上記媒体識別情報の正当性を検証し、上記検査データ生成部により生成された媒体識別情報検査データと検証された正当な媒体識別情報に基づいて情報記録媒体に対する認証処理を行うことを特徴とする請求の範囲第 11 項記載の情報記録装置。

17. 上記認証処理部は、上記媒体識別情報の記録者のデジタル署名として、上記情報記録媒体の製造者のデジタル署名が記録された情報記録媒体に対して、上記製造者のデジタル署名に基づいて上記媒体識別情報の正当性を検証することを特徴とする請求の範囲第 16 項記載の情報記録装置。

18. 上記認証処理部は、記録者についてのリボケーションリストが上記認証データとともに記録された情報記録媒体に対し、上記リボケーションリストに基づいて認証処理を行うことを特徴とする請求の範囲第 16 項記載の情報記録装置。

19. 上記認証処理部は、上記リボケーションリストを格納する記憶部を有し、情報記録媒体に記録されているリボケーションリストが正当なものであり、上記記憶部に格納されているリボケーションリストよりも新しい場合には、上記情報記録媒体に記録されているリボケーションリストを上記記憶部に格納し、上記記憶手段に格納したリボケーションリストに基づいて認証処理を行うことを特徴

とする請求の範囲第 18 項記載の情報記録装置。

20. ランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部と、上記ランダムパターン情報記録部から検出されるランダムパターン情報に基づいて生成された媒体識別情報を認証データとして格納した認証データ記録部とを有する情報記録媒体から情報を再生する情報再生装置であって、

情報記録媒体上のランダムパターン情報記録部からランダムパターン情報を検出するランダムパターン情報検出部と、

上記ランダムパターン情報検出部により検出されたランダムパターン情報から媒体識別情報検査データを生成する検査データ生成部と、

情報記録媒体上の認証データ記録部から認証データを読み出し、上記検査データ生成部により生成された媒体識別情報検査データと上記認証データに基づいて情報記録媒体に対する認証処理を行う認証処理部と、

情報を情報記録媒体から読み出す制御を行う再生制御部とを具備することを特徴とする情報再生装置。

21. 上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、情報の復号の処理を行う復号処理部を更に具備し、

上記再生制御部は、暗号化された情報を、上記認証された情報記録媒体から読み出す制御を行い、

上記復号処理部は、上記再生制御部によって情報記録媒体から読み出された暗号化された情報を、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、復号する処理を行うことを特徴とする請求の範囲第 20 項記載の情報再生装置。

22. 上記再生制御部は、暗号化された情報と前記情報の暗号化に用いた暗号鍵とを上記認証された情報記録媒体から読み出す制御を行うことを特徴とする請求の範囲第21項記載の情報再生装置。

23. 上記再生制御部は、暗号化された情報と暗号化された前記暗号鍵とを上記認証された情報記録媒体から読み出す制御を行い、

上記復号処理部は、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、読み出された暗号化された暗号化鍵を復号するとともに、上記暗号化された情報を復号された暗号化鍵を用いて暗号化された情報を復号する処理を行うことを特徴とする請求の範囲第22項記載の情報再生装置。

24. 上記認証処理部は、上記媒体識別情報が該媒体識別情報を記録した記録者のデジタル署名とともに認証データとして記録された情報記録媒体に対し、上記記録者のデジタル署名に基づいて上記媒体識別情報の正当性を検証し、上記検査データ生成部により生成された媒体識別情報検査データと検証された正当な媒体識別情報に基づいて情報記録媒体に対する認証処理を行うことを特徴とする請求の範囲第20項記載の情報再生装置。

25. 上記認証処理部は、上記媒体識別情報の記録者のデジタル署名として、上記情報記録媒体の製造者のデジタル署名が記録された情報記録媒体に対して、上記製造者のデジタル署名に基づいて上記媒体識別情報の正当性を検証することを特徴とする請求の範囲第24項記載の情報再生装置。

26. 上記認証処理部は、記録者についてのリボケーションリストが上記認証データとともに記録された情報記録媒体に対し、上記リボケーションリストに基づいて認証処理を行うことを特徴とする

請求の範囲第 2 4 項記載の情報再生装置。

27. 上記認証処理部は、上記リボケーションリストを格納する記憶部を有し、情報記録媒体に記録されていたリボケーションリストが正当なものであり、上記記憶部に格納されているリボケーションリストよりも新しい場合には、上記情報記録媒体に記録されていたリボケーションリストを上記記憶部に格納し、上記記憶部に格納したリボケーションリストに基づいて認証処理を行うことを特徴とする請求の範囲第 2 6 項記載の情報再生装置。

28. 情報記録媒体に認証のための情報を記録する認証データ記録装置において、

ランダムな物理現象によるランダムパターン情報が記録された情報記録媒体上のランダムパターン情報記録部から上記ランダムパターン情報を検出するランダムパターン情報検出部と、

上記ランダムパターン情報検出部により検出された上記ランダムパターン情報から媒体識別情報を生成する媒体識別情報生成部と、

上記媒体識別情報生成部により生成した媒体識別情報を認証データとして上記情報記録媒体上の認証データ記録部に記録する制御を行う認証データ記録制御部と

を具備することを特徴とする認証データ記録装置。

29. 上記認証データ記録制御部は、上記媒体識別情報を該媒体識別情報の記録者のデジタル署名とともに認証データとして上記情報記録媒体上の認証データ記録部に記録することを特徴とする請求の範囲第 2 8 項記載の認証データ記録装置。

30. 上記認証データ記録制御部は、上記媒体識別情報の記録者のデジタル署名として、上記情報記録媒体の製造者のデジタル署名



を記録することを特徴とする請求の範囲第 28 項記載の認証データ記録装置。

31. 上記認証データ記録制御部は、上記情報記録媒体上の認証データ記録部に製造者についてのリボケーションリストを上記認証データとともに記録することを特徴とする請求の範囲第 28 項記載の認証データ記録装置。

32. 情報記録媒体に対する認証処理を行う認証処理装置において、

情報記録媒体上のランダムパターン情報記録部からランダムパターン情報を検出するランダムパターン情報検出部と、

上記ランダムパターン情報検出部により検出されたランダムパターン情報から媒体識別情報検査データを生成する検査データ生成部と、

情報記録媒体上の認証データ記録部から認証データを再生し、上記検査データ生成部により生成された媒体識別情報検査データと上記認証データに基づいて情報記録媒体に対する認証処理を行う認証処理部と

を具備することを特徴とする認証処理装置。

33. 上記認証処理部は、上記媒体識別情報が該媒体識別情報を記録した記録者のデジタル署名とともに認証データとして記録された情報記録媒体に対し、上記記録者のデジタル署名に基づいて上記媒体識別情報の正当性を検証し、上記検査データ生成部により生成された媒体識別情報検査データと検証された正当な媒体識別情報に基づいて情報記録媒体に対する認証処理を行うことを特徴とする請求の範囲第 32 項記載の認証処理装置。

34. 上記認証処理部は、上記媒体識別情報の記録者のデジタル署名として、上記情報記録媒体の製造者のデジタル署名が記録された情報記録媒体に対して、上記製造者のデジタル署名に基づいて上記媒体識別情報の正当性を検証することを特徴とする請求の範囲第33項記載の認証処理装置。

35. 上記認証処理部は、記録者についてのリボケーションリストが上記認証データとともに記録された情報記録媒体に対し、上記リボケーションリストに基づいて認証処理を行うことを特徴とする請求の範囲第33項記載の認証処理装置。

36. 上記認証処理部は、上記リボケーションリストを格納する記憶部を有し、情報記録媒体に記録されていたリボケーションリストが正当なものであり、上記記憶部に格納されているリボケーションリストよりも新しい場合には、上記情報記録媒体に記録されていたリボケーションリストを上記記憶部に格納し、上記記憶部に格納したリボケーションリストに基づいて認証処理を行うことを特徴とする請求の範囲第35項記載の認証処理装置。

37. 上記認証処理部は、記憶部を有し、扱った情報記録媒体の記録者の識別情報とその公開鍵をリボケーションフラグとともに記憶しておき、新しいリボケーションリストを用いてリボケーションフラグを更新し、上記記憶部に格納したリボケーションリストに基づいて認証処理を行うことを特徴とする請求の範囲第35項記載の認証処理装置。

38. 情報を記録し、再生する情報記録再生方法であって、  
情報記録媒体上のランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部からランダムな物理現象

によるランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報を生成して、上記媒体識別情報を認証データとして上記情報記録媒体上の認証データ記録部に記録する制御を行う認証データ記録制御工程と、

上記ランダムパターン情報記録部から上記ランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報検査データを生成するとともに、上記情報記録媒体上の認証データ記録部から認証データを読み出し、上記ランダムパターン情報から生成した媒体識別情報検査データと上記認証データに基づいて上記情報記録媒体に対する認証処理を行う認証処理工程と、

上記認証処理工程の認証結果に基づいて、情報記録媒体への情報記録及び情報記録媒体からの情報再生の制御を行う情報記録再生制御工程と

を具備することを特徴とする情報記録再生方法。

39. 上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、情報の暗号化の処理を行う暗号処理工程を更に具備し、

上記情報記録再生制御工程は、上記暗号処理工程で暗号化された情報を、上記認証された情報記録媒体に記録する制御を行うことを特徴とする請求の範囲第38項記載の情報記録再生方法。

40. 上記情報記録再生制御工程は、暗号化した情報と前記情報の暗号化に用いた暗号鍵とを上記認証された情報記録媒体に記録する制御を行うことを特徴とする請求の範囲第39項記載の情報記録再生方法。

41. 上記暗号処理工程は、上記暗号化鍵を用いて情報を暗号化するとともに、上記認証処理により認証された情報記録媒体の媒体

識別情報を用いて、上記情報の暗号化に用いた暗号鍵を暗号化し、

上記情報記録再生制御工程は、上記暗号鍵により暗号化された情報と上記暗号化された暗号鍵とを上記認証された情報記録媒体に記録する制御を行うことを特徴とする請求の範囲第40項記載の情報記録再生方法。

42. 上記暗号処理工程は、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、上記情報の暗号化に用いる暗号鍵を生成することを特徴とする請求の範囲第39項記載の情報記録再生方法。

43. 上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、情報の復号の処理を行う復号処理工程を更に具備し、

上記情報記録再生制御工程は、暗号化された情報を、上記認証された情報記録媒体から読み出す制御を行い、

上記復号処理工程は、上記情報記録再生制御工程によって情報記録媒体から読み出された暗号化された情報を、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、復号する処理を行うことを特徴とする請求の範囲第38項記載の情報記録再生方法。

44. 上記情報記録再生制御工程は、暗号化された情報と前記情報の暗号化に用いた暗号鍵とを上記認証された情報記録媒体から読み出す制御を行うことを特徴とする請求の範囲第43項記載の情報記録再生方法。

45. 上記情報記録再生制御工程は、暗号化された情報と暗号化された前記暗号鍵とを上記認証された情報記録媒体から読み出す制御を行い、

上記復号処理工程は、上記認証処理により認証された情報記録媒

体の媒体識別情報を用いて、読み出された暗号化された暗号化鍵を復号するとともに、上記暗号化され情報を復号された暗号化鍵を用いて暗号化された情報を復号する処理を行うことを特徴とする請求の範囲第44項記載の情報記録再生方法。

46. 上記認証データ記録制御工程は、上記媒体識別情報を該媒体識別情報の記録者のデジタル署名とともに認証データとして上記情報記録媒体上の認証データ記録部に記録することを特徴とする請求の範囲第38項記載の情報記録再生方法。

47. 上記認証データ記録制御工程は、上記媒体識別情報の記録者のデジタル署名として、上記情報記録媒体の製造者のデジタル署名を記録することを特徴とする請求の範囲第46項記載の情報記録再生方法。

48. ランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部と、上記ランダムパターン情報記録部から検出されるランダムパターン情報に基づいて生成された媒体識別情報を認証データとして格納した認証データ記録部とを有する情報記録媒体に情報を記録する情報記録方法であって、

情報記録媒体上のランダムパターン情報記録部からランダムパターン情報を検出するランダムパターン情報検出工程と、

上記ランダムパターン情報検出工程により検出されたランダムパターン情報から媒体識別情報検査データを生成する検査データ生成工程と、

情報記録媒体上の認証データ記録部から認証データを読み出し、上記検査データ生成工程により生成された媒体識別情報検査データと上記認証データに基づいて、情報記録媒体に対する認証処理を行

い、認証結果に基づいて情報の情報記録媒体への書き込みの可否を制御する認証処理工程と、

情報を情報記録媒体に記録する制御を行う記録制御工程とを具備することを特徴とする情報記録方法。

49. 上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、情報の暗号化の処理を行う暗号処理工程を更に具備し、

上記記録制御工程は、上記暗号処理工程で暗号化された情報を、上記認証された情報記録媒体に記録する制御を行うことを特徴とする請求の範囲第48項記載の情報記録方法。

50. 上記記録制御工程は、暗号化した情報と前記情報の暗号化に用いた暗号鍵とを上記認証された情報記録媒体に記録する制御を行うことを特徴とする請求の範囲第49項記載の情報記録方法。

51. 上記暗号処理工程は、上記暗号化鍵を用いて情報を暗号化するとともに、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、上記情報の暗号化に用いた暗号鍵を暗号化し、

上記記録制御工程は、上記暗号鍵により暗号化された情報と上記暗号化された暗号鍵とを上記認証された情報記録媒体に記録する制御を行うことを特徴とする請求の範囲第50項記載の情報記録方法。

52. 上記暗号処理工程は、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、上記情報の暗号化に用いる暗号鍵を生成することを特徴とする請求の範囲第49項記載の情報記録方法。

53. 上記認証処理工程は、上記媒体識別情報が該媒体識別情報を記録した記録者のデジタル署名とともに認証データとして記録された情報記録媒体に対し、上記記録者のデジタル署名に基づいて上

記媒体識別情報の正当性を検証し、上記検査データ生成工程により生成された媒体識別情報検査データと検証された正当な媒体識別情報に基づいて情報記録媒体に対する認証処理を行うことを特徴とする請求の範囲第48項記載の情報記録方法。

54. 上記認証処理工程は、上記媒体識別情報の記録者のデジタル署名として上記情報記録媒体の製造者のデジタル署名が記録された情報記録媒体に対し、上記製造者のデジタル署名に基づいて上記媒体識別情報の正当性を検証することを特徴とする請求の範囲第53項記載の情報記録方法。

55. 上記認証処理工程は、記録者についてのリボケーションリストが上記認証データとともに記録された情報記録媒体に対し、上記リボケーションリストに基づいて認証処理を行うことを特徴とする請求の範囲第53項記載の情報記録方法。

56. 上記認証処理工程は、情報記録媒体に記録されているリボケーションリストが正当なものであり、既に格納されているリボケーションリストよりも新しい場合には、上記情報記録媒体に記録されているリボケーションリストを格納し、上記新たに格納したリボケーションリストに基づいて認証処理を行うことを特徴とする請求の範囲第55項記載の情報記録方法。

57. ランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部と、上記ランダムパターン情報記録部から検出されるランダムパターン情報に基づいて生成された媒体識別情報を認証データとして格納した認証データ記録部とを有する情報記録媒体から情報を再生する情報再生方法であって、

情報記録媒体上のランダムパターン情報記録部からランダムパタ

ン情報を検出するランダムパターン情報検出工程と、

上記ランダムパターン情報検出工程により検出されたランダムパターン情報から媒体識別情報検査データを生成する検査データ生成工程と、

情報記録媒体上の認証データ記録部から認証データを読み出し、上記検査データ生成工程により生成された媒体識別情報検査データと上記認証データに基づいて情報記録媒体に対する認証処理を行う認証処理工程と、

情報を情報記録媒体から読み出す制御を行う再生制御工程とを具備することを特徴とする情報再生方法。

58. 上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、情報の復号の処理を行う復号処理工程を更に具備し、

上記再生制御工程は、暗号化された情報を、上記認証された情報記録媒体から読み出す制御を行い、

上記復号処理工程は、上記再生制御工程によって情報記録媒体から読み出された暗号化された情報を、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、復号する処理を行うことを特徴とする請求の範囲第57項記載の情報再生方法。

59. 上記再生制御工程は、暗号化された情報と前記情報の暗号化に用いた暗号鍵とを上記認証された情報記録媒体から読み出す制御を行うことを特徴とする請求の範囲第58項記載の情報再生方法。

60. 上記再生制御工程は、暗号化された情報と暗号化された前記暗号鍵とを上記認証された情報記録媒体から読み出す制御を行い、

上記復号処理工程は、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、読み出された暗号化された暗号化鍵を



復号するとともに、上記暗号化され情報を復号された暗号化鍵を用いて暗号化された情報を復号する処理を行うことを特徴とする請求の範囲第59項記載の情報再生方法。

61. 上記認証処理工程は、上記媒体識別情報が該媒体識別情報を記録した記録者のデジタル署名とともに認証データとして記録された情報記録媒体に対し、上記記録者のデジタル署名に基づいて上記媒体識別情報の正当性を検証し、上記検査データ生成工程により生成された媒体識別情報検査データと検証された正当な媒体識別情報に基づいて情報記録媒体に対する認証処理を行うことを特徴とする請求の範囲第57項記載の情報再生方法。

62. 上記認証処理工程は、上記媒体識別情報の記録者のデジタル署名として、上記情報記録媒体の製造者のデジタル署名が記録された情報記録媒体に対して、上記製造者のデジタル署名に基づいて上記媒体識別情報の正当性を検証することを特徴とする請求の範囲第61項記載の情報再生方法。

63. 上記認証処理工程は、記録者についてのリボケーションリストが上記認証データとともに記録された情報記録媒体に対し、上記リボケーションリストに基づいて認証処理を行うことを特徴とする請求の範囲第61項記載の情報再生方法。

64. 上記認証処理工程は、情報記録媒体に記録されていたリボケーションリストが正当なものであり、既に格納されているリボケーションリストよりも新しい場合には、上記情報記録媒体に記録されていたリボケーションリストを格納し、新たに格納したリボケーションリストに基づいて認証処理を行うことを特徴とする請求の範囲第63項記載の情報再生方法。

65. 情報記録媒体に認証のための情報を記録する認証データ記録方法において、

ランダムな物理現象によるランダムパターン情報が記録された情報記録媒体上のランダムパターン情報記録部から上記ランダムパターン情報を検出するランダムパターン情報検出工程と、

上記ランダムパターン情報検出工程により検出された上記ランダムパターン情報から媒体識別情報を生成する媒体識別情報生成工程と、

上記媒体識別情報生成工程により生成した媒体識別情報を認証データとして上記情報記録媒体上の認証データ記録部に記録する制御を行う認証データ記録制御工程と

を具備することを特徴とする認証データ記録方法。

66. 上記認証データ記録制御工程は、上記媒体識別情報を該媒体識別情報の記録者のデジタル署名とともに認証データとして上記情報記録媒体上の認証データ記録部に記録することを特徴とする請求の範囲第65項記載の認証データ記録方法。

67. 上記認証データ記録制御工程は、上記媒体識別情報の記録者のデジタル署名として、上記情報記録媒体の製造者のデジタル署名を記録することを特徴とする請求の範囲第66項記載の認証データ記録方法。

68. 上記認証データ記録制御工程は、上記情報記録媒体上の認証データ記録部に製造者についてのリボケーションリストを上記認証データとともに記録することを特徴とする請求の範囲第65項記載の認証データ記録方法。

69. 情報記録媒体に対する認証処理を行う認証処理方法におい

て、

情報記録媒体上のランダムパターン情報記録部からランダムパターン情報を検出するランダムパターン情報検出工程と、

上記ランダムパターン情報検出工程により検出されたランダムパターン情報から媒体識別情報検査データを生成する検査データ生成工程と、

情報記録媒体上の認証データ記録部から認証データを再生し、上記検査データ生成工程により生成された媒体識別情報検査データと上記認証データに基づいて情報記録媒体に対する認証処理を行う認証処理工程と

を具備することを特徴とする認証処理方法。

70. 上記認証処理工程は、上記媒体識別情報が該媒体識別情報を記録した記録者のデジタル署名とともに認証データとして記録された情報記録媒体に対し、上記記録者のデジタル署名に基づいて上記媒体識別情報の正当性を検証し、上記検査データ生成工程により生成された媒体識別情報検査データと検証された正当な媒体識別情報に基づいて情報記録媒体に対する認証処理を行うことを特徴とする請求の範囲第69項記載の認証処理方法。

71. 上記認証処理工程は、上記媒体識別情報の記録者のデジタル署名として上記情報記録媒体の製造者のデジタル署名が記録された情報記録媒体に対し、上記製造者のデジタル署名に基づいて上記媒体識別情報の正当性を検証することを特徴とする請求の範囲第70項記載の認証処理方法。

72. 上記認証処理工程は、記録者についてのリボケーションリストが上記認証データとともに記録された情報記録媒体に対し、上

記リボケーションリストに基づいて認証処理を行うことを特徴とする請求の範囲第70項記載の認証処理方法。

73. 上記認証処理工程は、情報記録媒体に記録されていたリボケーションリストが正当なものであり、既に格納されているリボケーションリストよりも新しい場合には、上記情報記録媒体に記録されていたリボケーションリストを格納し、新たに格納したリボケーションリストに基づいて認証処理を行うことを特徴とする請求の範囲第72項記載の認証処理方法。

74. 上記認証処理工程は、扱った情報記録媒体の記録者の識別情報とその公開鍵をリボケーションフラグとともに記憶しておき、新しいリボケーションリストを用いてリボケーションフラグを更新し、上記記憶工程に格納したリボケーションリストに基づいて認証処理を行うことを特徴とする請求の範囲第72項記載の認証処理方法。

75. 情報が記録される情報記録媒体において、

ランダムな物理現象によるランダムパターン情報が記録されたランダムパターン情報記録部と、

上記ランダムパターン情報記録部から検出されるランダムパターン情報に基づいて生成された媒体識別情報が認証データとして記録された認証データ記録部と、

情報が記録される情報記録部と

を具備することを特徴とする情報記録媒体。

76. 上記認証データ記録部には、上記媒体識別情報が、該媒体識別情報の記録者のデジタル署名とともに認証データとして記録されていることを特徴とする請求の範囲第75項記載の情報記録媒体。

77. 上記認証データ記録部には、上記媒体識別情報の記録者のデジタル署名として、上記情報記録媒体の製造者のデジタル署名が記録されていることを特徴とする請求の範囲第76項記載の情報記録媒体。

78. 上記認証データ記録部には、製造者についてのリボケーションリストが上記認証データとともに記録されていることを特徴とする請求の範囲第77項記載の情報記録媒体。

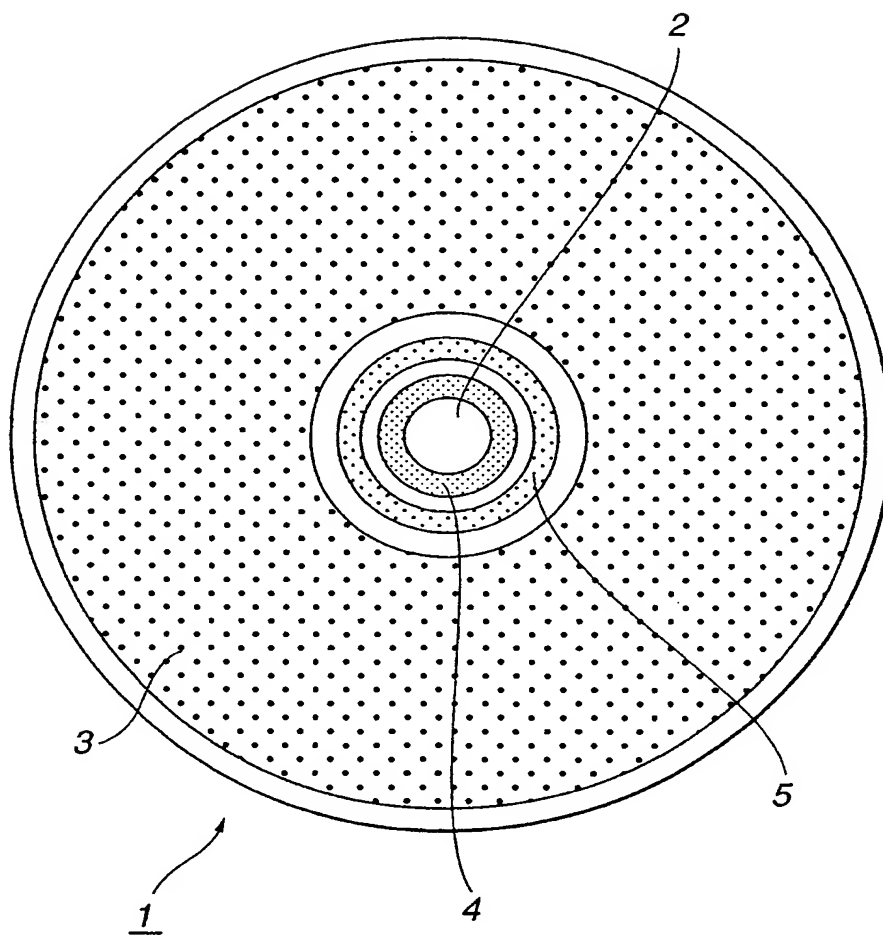


FIG.1

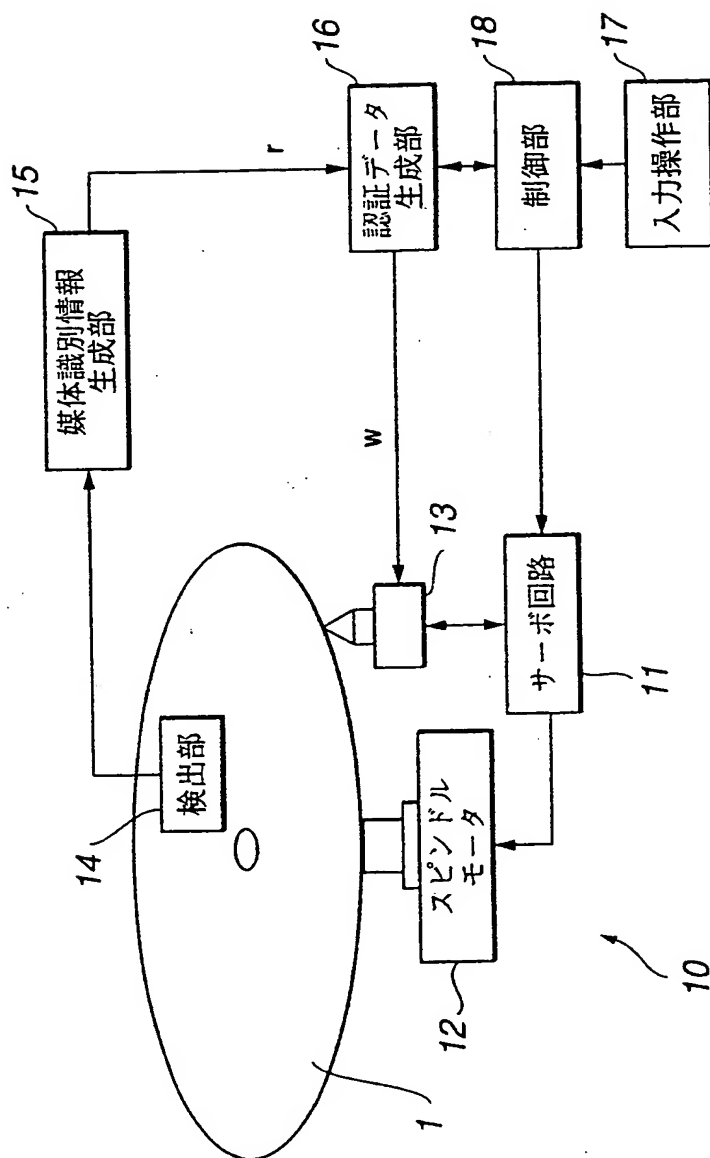


FIG.2

3/14

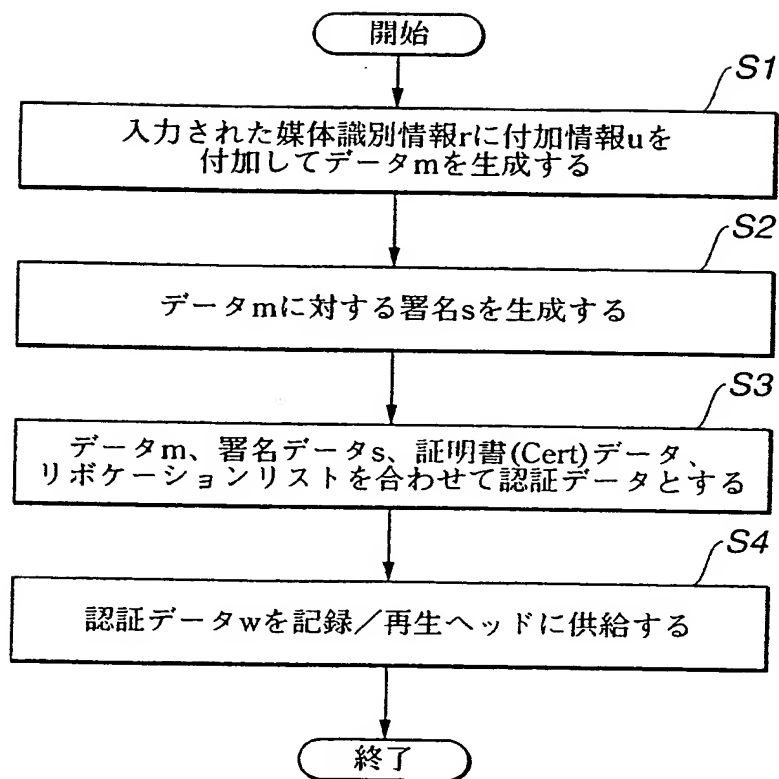


FIG.3



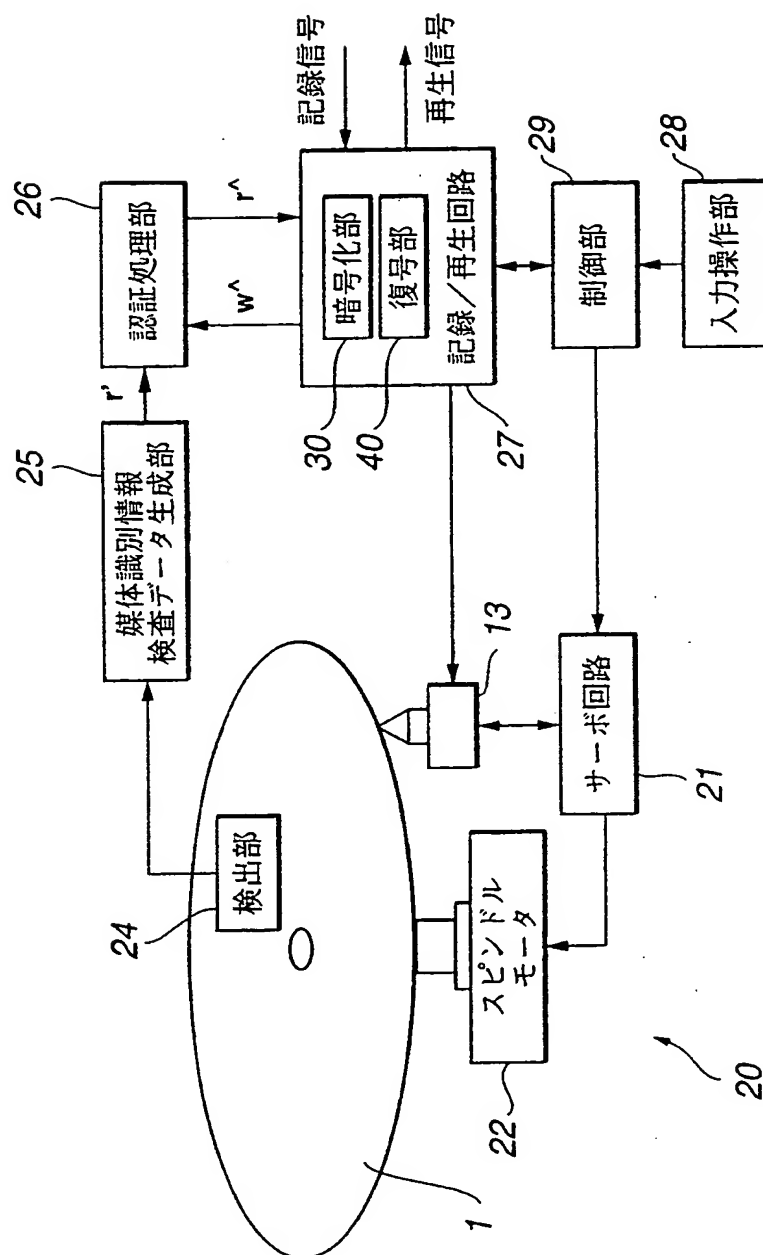


FIG.4

5/14

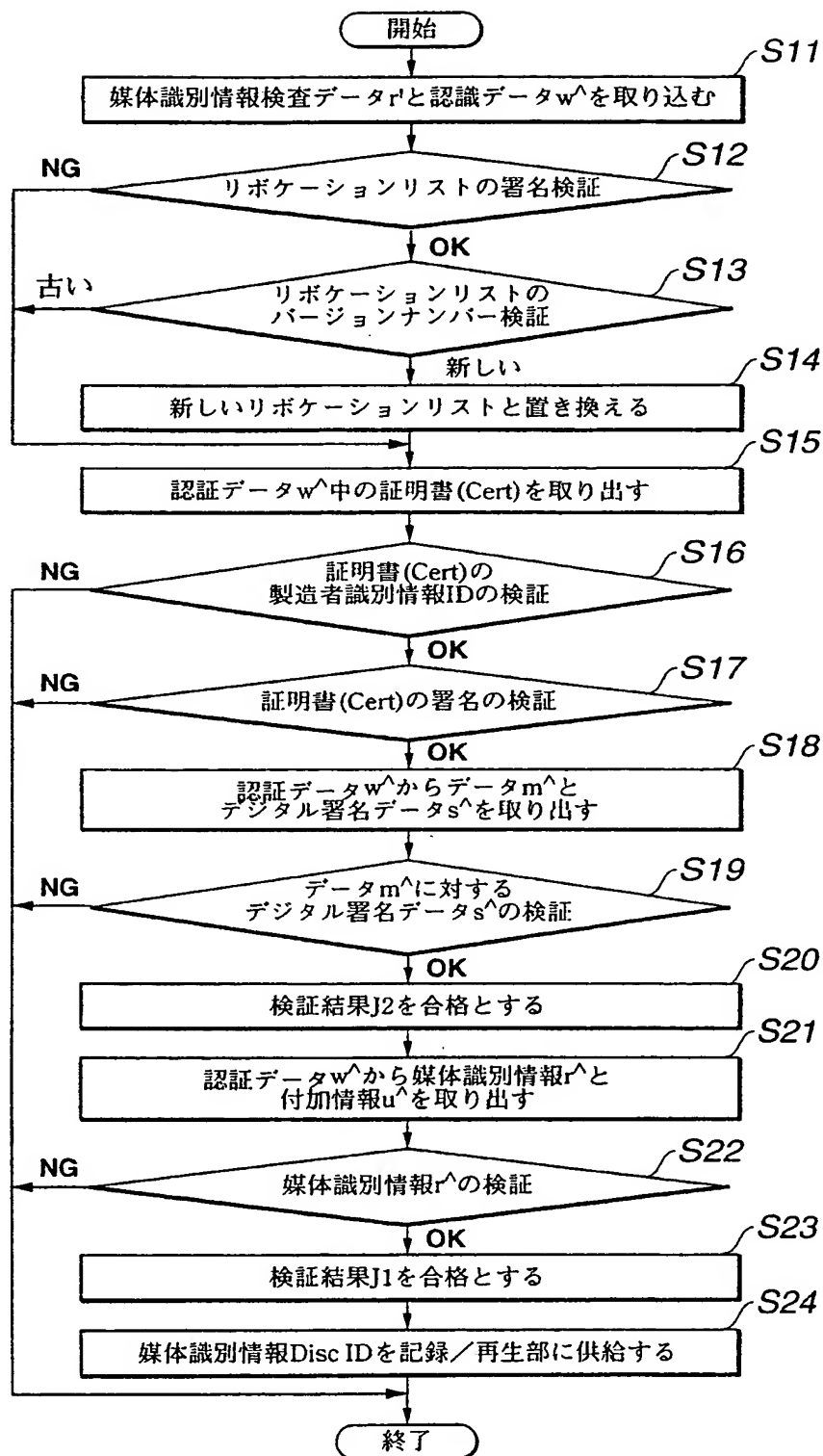


FIG.5

6/14

リボケーションリスト

バージョンナンバー
製造者ID
...

FIG.6

公開鍵リスト

最新のリボケーションリストのバージョンナンバー		
製造者ID	公開鍵	リボケーションフラグ(YES/NO)
...	...	...

FIG.7

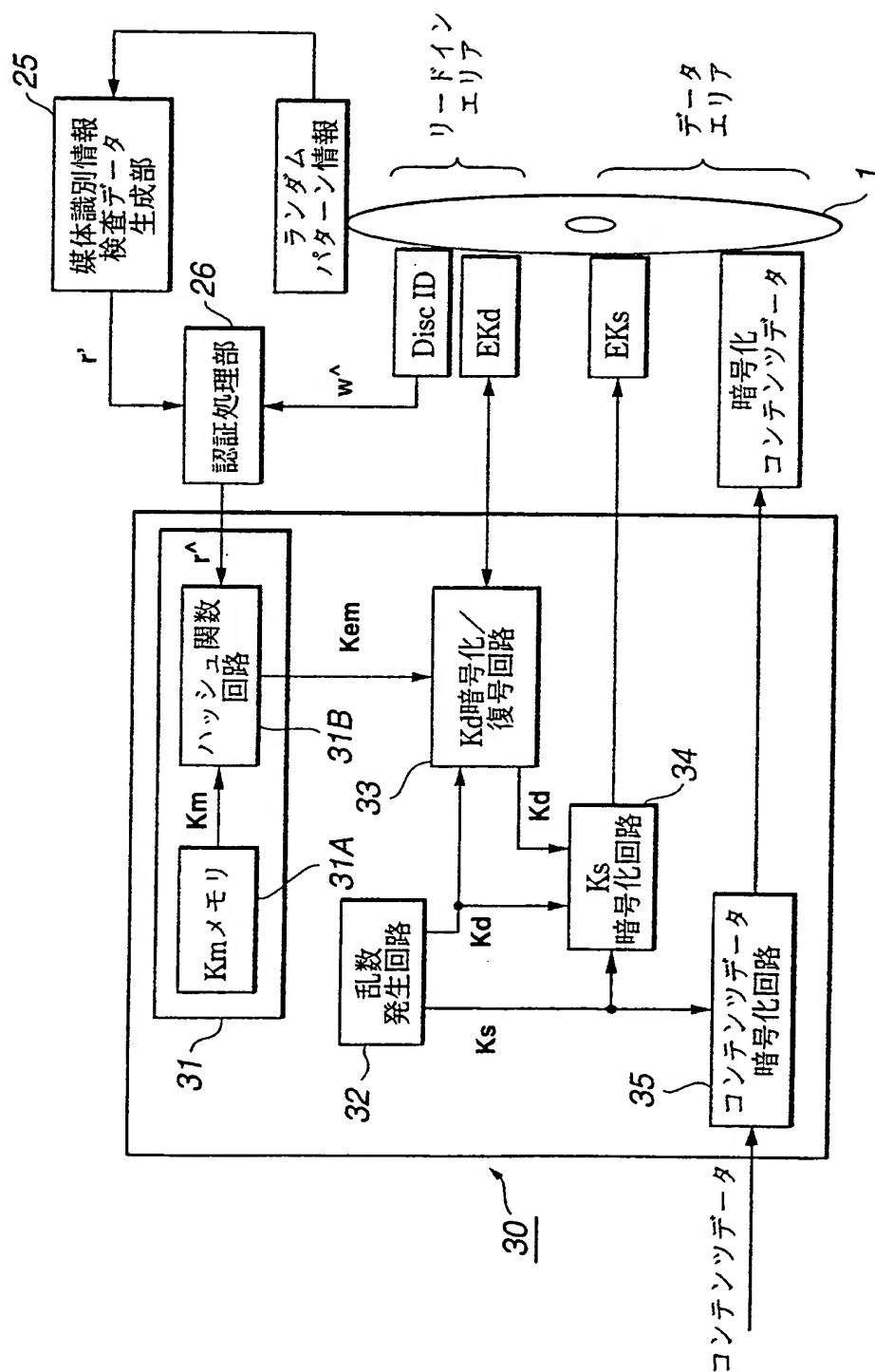


FIG.8

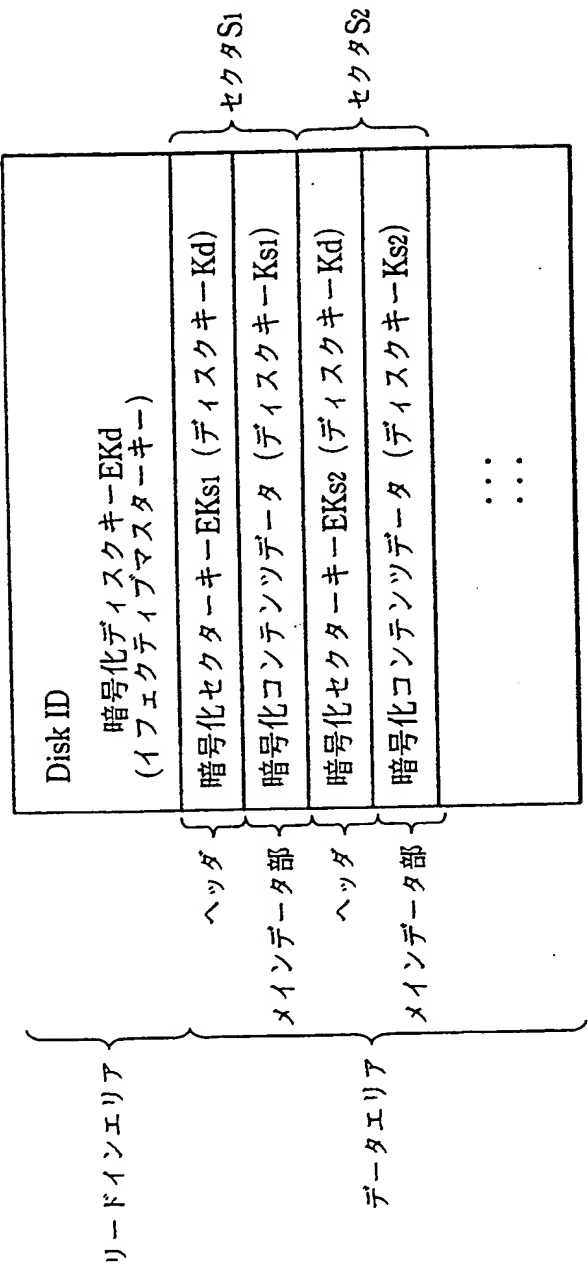


FIG.9

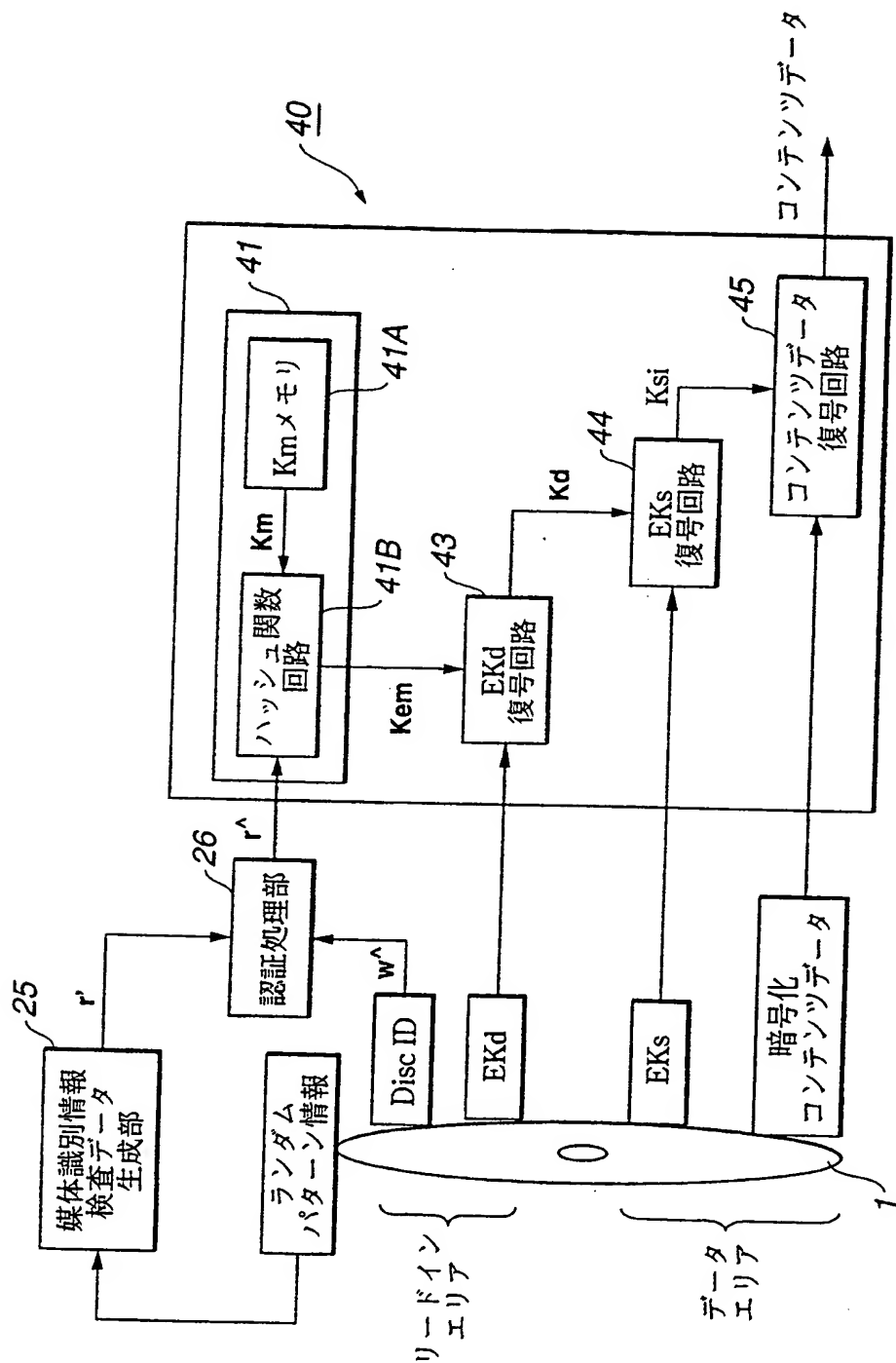


FIG.10

10/14

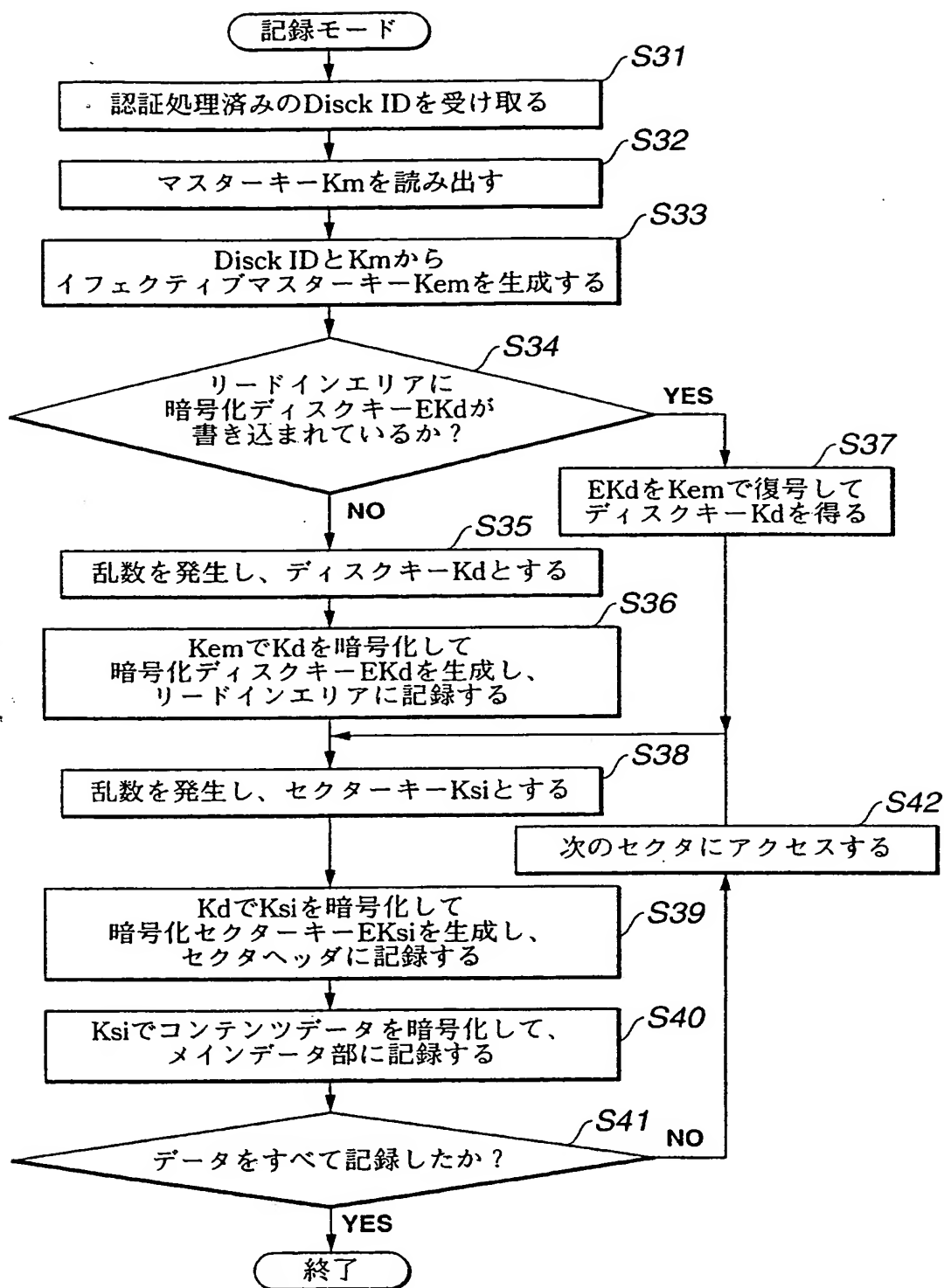


FIG.11

11/14

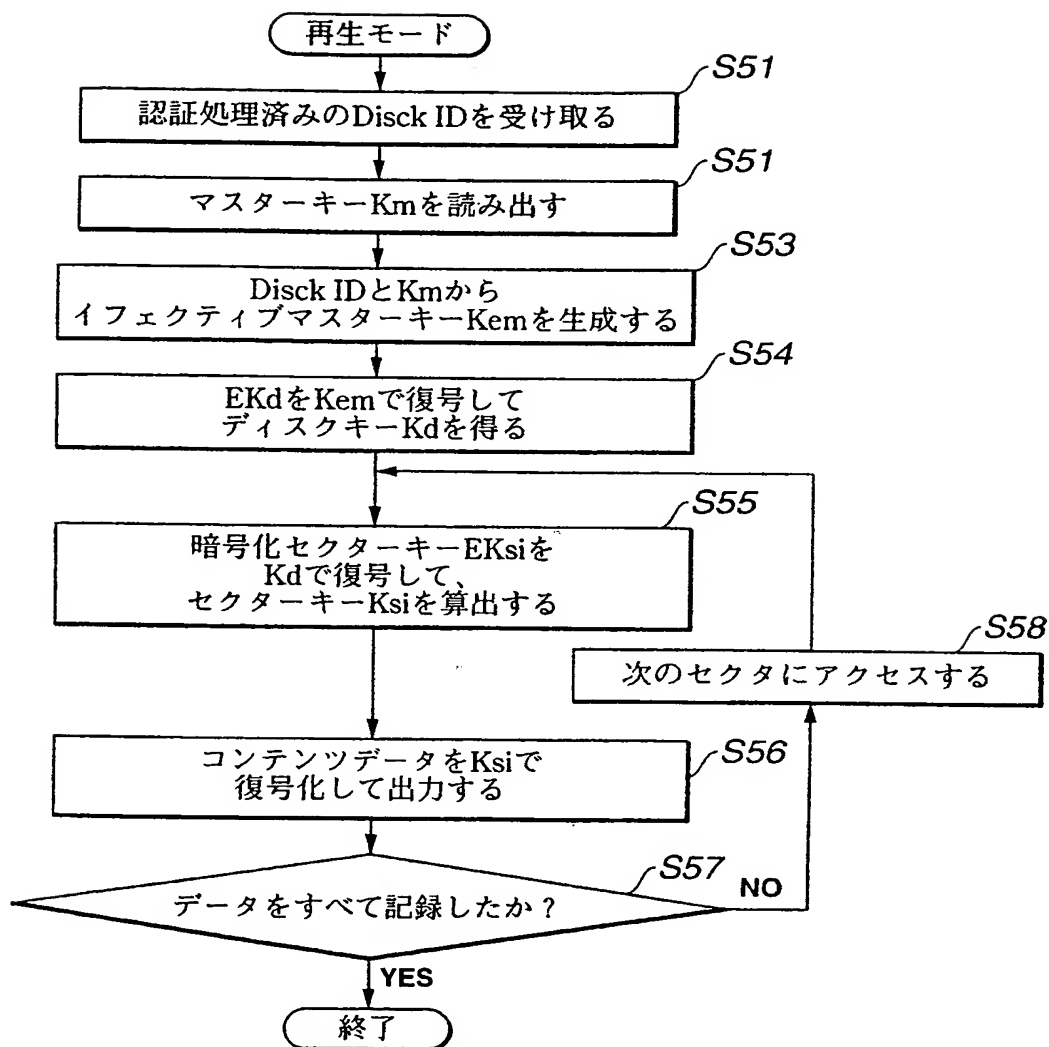


FIG.12



12/14

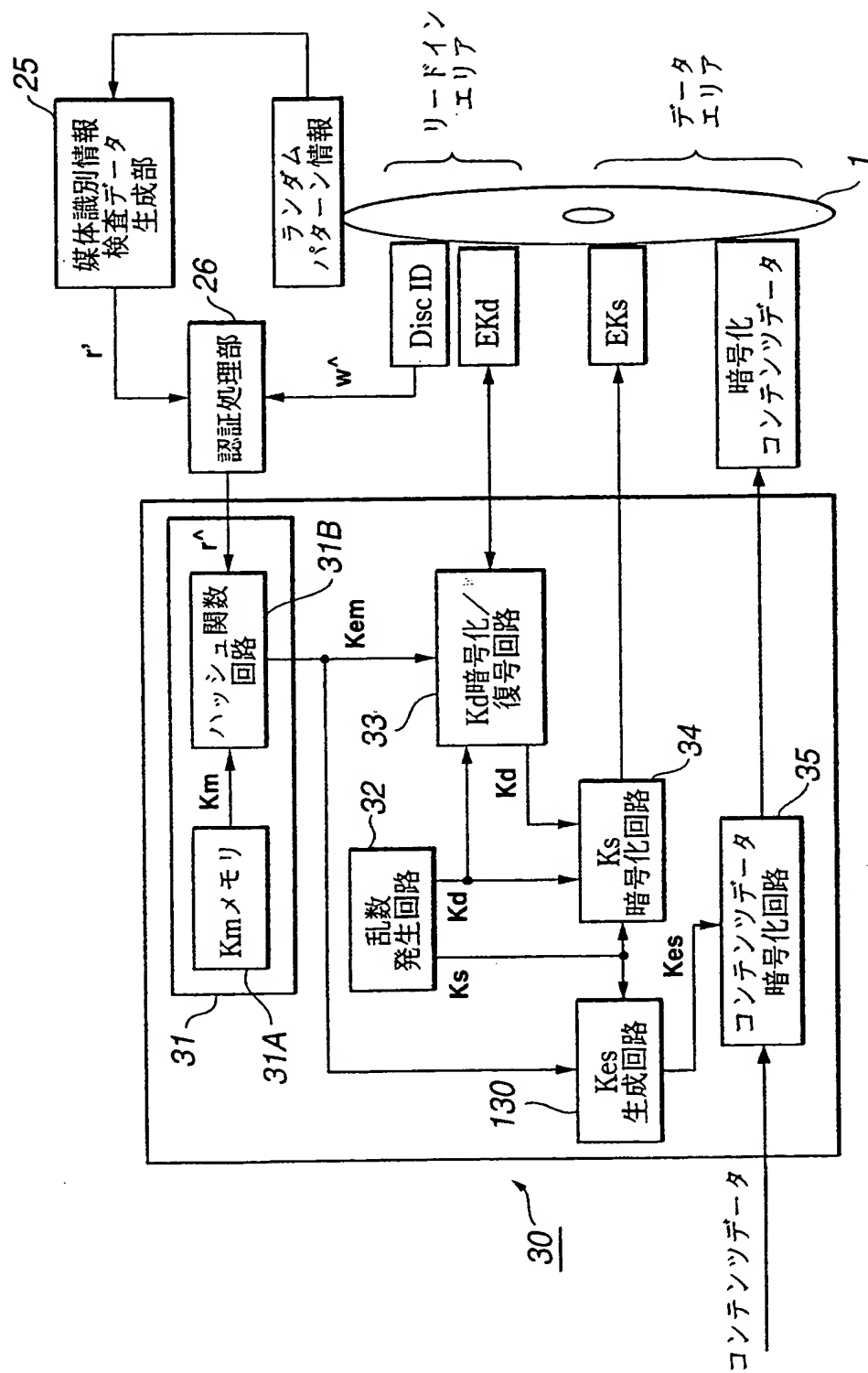


FIG.13

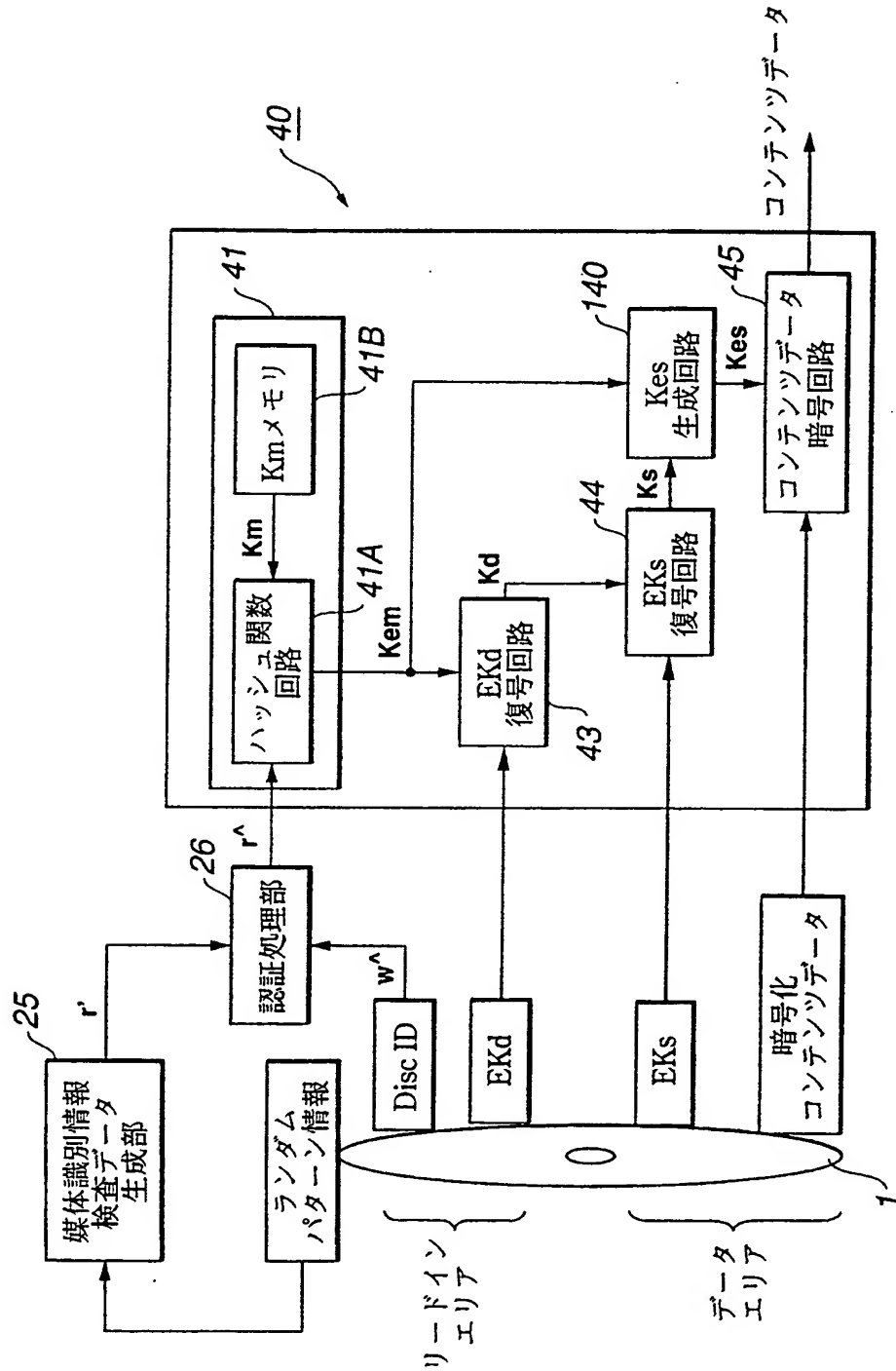


FIG.14

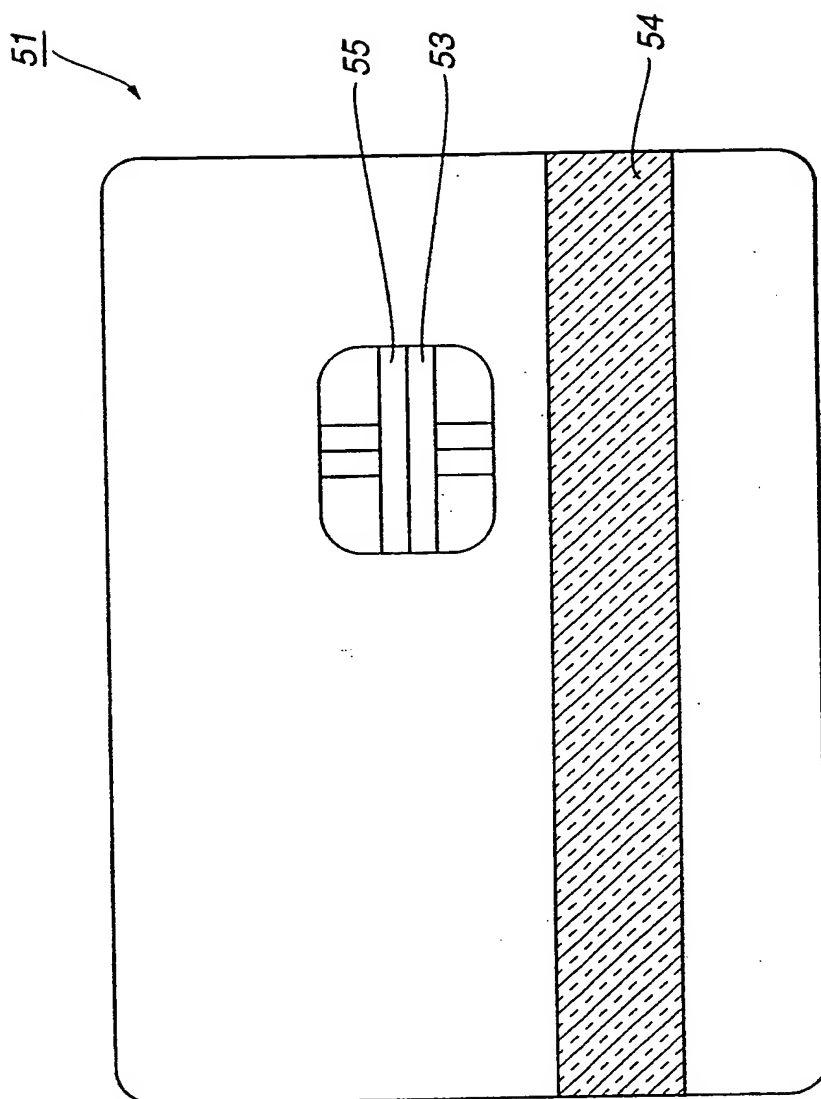


FIG.15

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/00658

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl<sup>7</sup> G11B20/10

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G11B20/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2000
Kokai Jitsuyo Shinan Koho	1971-2000	Jitsuyo Shinan Toroku Koho	1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 7-182766, A (Matsushita Electric Ind. Co., Ltd.), 21 July, 1995 (21.07.95), Full text; Figs. 1 to 16 (Family: none)	1-78
A	JP, 10-21144, A (Hitachi, Ltd.), 23 January, 1998 (23.01.98), Full text; Figs. 1 to 10 (Family: none)	1-78
A	JP, 11-7412, A (Oputoromu K.K.), 12 January, 1999 (12.01.99), Full text; Figs. 1 to 3 & AU, 8034498, A	1-78

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

\* Special categories of cited documents:  
 "A" document defining the general state of the art which is not considered to be of particular relevance  
 "E" earlier document but published on or after the international filing date  
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)  
 "O" document referring to an oral disclosure, use, exhibition or other means  
 "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone  
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art  
 "&" document member of the same patent family

Date of the actual completion of the international search  
25 April, 2000 (25.04.00)Date of mailing of the international search report  
02 May, 2000 (02.05.00)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## 国際調査報告

国際出願番号 PCT/J P00/00658

A. 発明の属する分野の分類 (国際特許分類 (IPC))  
Int. Cl. G11B20/10

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))  
Int. Cl. G11B20/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年  
日本国公開実用新案公報 1971-2000年  
日本国登録実用新案公報 1994-2000年  
日本国実用新案登録公報 1996-2000年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	J P, 7-182766, A (松下電器産業株式会社) 21. 7. 1995 (21. 07. 95) 全文, 第1-16図 (ファミリーなし)	1-78
A	J P, 10-21144, A (株式会社日立製作所) 23. 1月. 1998 (23. 01. 98) 全文, 第1-10図 (ファミリーなし)	1-78
A	J P, 11-7412, A (株式会社オプトロム) 12. 1月. 1999 (12. 01. 99) 全文, 第1-3図 & AU, 8034498, A	1-78

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に言及する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」 同一パテントファミリー文献

国際調査を完了した日

25. 04. 00

国際調査報告の発送日

02.05.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)  
郵便番号 100-8915  
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

小松 正

5Q

7736

電話番号 03-3581-1101 内線 6922

**THIS PAGE BLANK (USPTO)**

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

**THIS PAGE BLANK (USPTO)**